EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 1 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 1
Topic #: 1
[All SC-401 Questions]

DRAG DROP -

Case Study -

Instructions -
This is a case study. Case studies are not timed separately from other exam sections. You can use as much exam time as you would like to complete each case study. However, there might be additional case studies or other exam sections. Manage your time to ensure that you can complete all the exam sections in the time provided. Pay attention to the Exam Progress at the top of the screen so you have sufficient time to complete any exam sections that follow this case study.
To answer the case study questions, you will need to reference information that is provided in the case. Case studies and associated questions might contain exhibits or other resources that provide more information about the scenario described in the case. Information provided in an individual question does not apply to the other questions in the case study.
A Review Screen will appear at the end of this case study. From the Review Screen, you can review and change your answers before you move to the next exam section. After you leave this case study, you will NOT be able to return to it.

To start the case study -
To display the first question in this case study, select the "Next" button. To the left of the question, a menu provides links to information such as business requirements, the existing environment, and problem statements. Please read through all this information before answering any questions. When you are ready to answer a question, select the "Question" button to return to the question.

Overview -
Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.

Existing Environment -

Microsoft 365 Environment -
Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

Users store data in the following locations:

SharePoint sites -

OneDrive accounts -

Exchange email -

Exchange public folders -

Teams chats -

Teams channel messages -
When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

SharePoint Online Environment -
Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.
Site2 contains the files shown in the following table.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.
Site4 has the following two retention policies applied:

Name: Site4RetentionPolicy1 -
Locations to apply the policy: Site4
Delete items older than: 2 years
Delete content based on: When items were created

Name: Site4RetentionPolicy2 -
Locations to apply the policy: Site4
Retain items for a specific period: 4 years
Start the retention period based on: When items were created
At the end of the retention period: Do nothing

Problem Statements -
Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

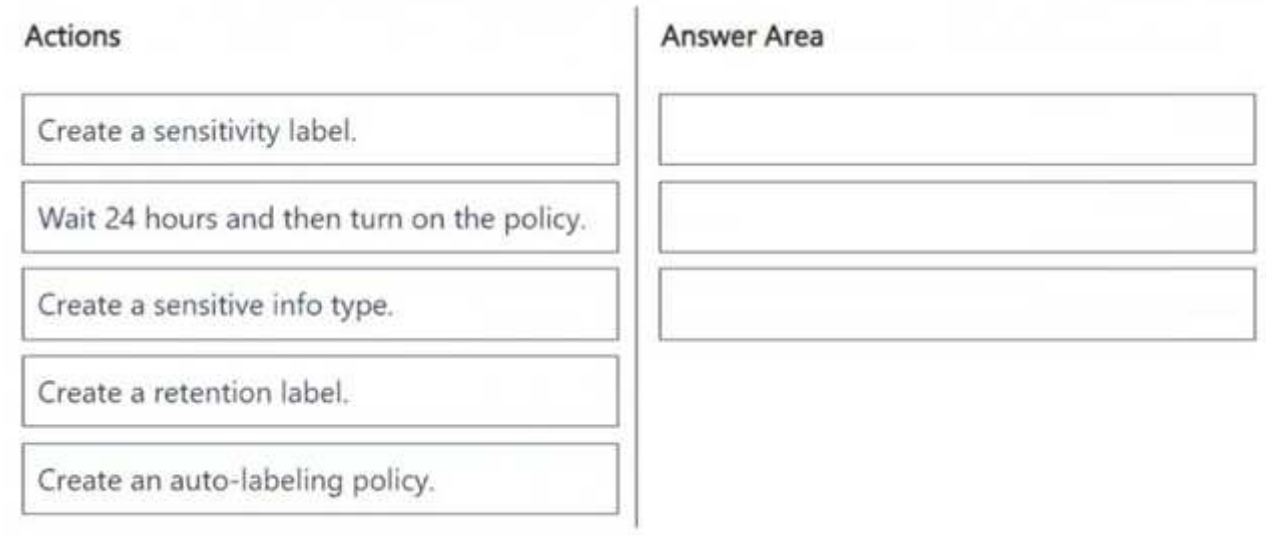
Requirements -

Planned Changes -
Contoso plans to create the following data loss prevention (DLP) policy:

Name: DLPpolicy1 -
Locations to apply the policy: Site2
Conditions:
Content contains any of these sensitive info types: SWIFT Code

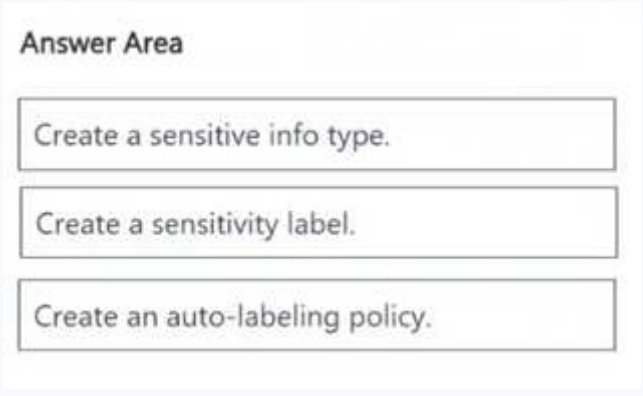
Instance count: 2 to any -
Actions: Restrict access to the content

Technical Requirements -
Contoso must meet the following technical requirements:
All administrative users must be able to review DLP reports.
Whenever possible, the principle of least privilege must be used.
For all users, all Microsoft 365 data must be retained for at least one year.
Confidential documents must be detected and protected by using Microsoft 365.
Site1 documents that include credit card numbers must be labeled automatically.
All administrative users must be able to create Microsoft 365 sensitivity labels.
After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.
You need to meet the technical requirements for the Site1 documents.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.


Actions
Answer Area
Create a sensitivity label.
Wait 24 hours and then turn on the policy.
Create a sensitive info type.
Create a retention label.
Create an auto-labeling policy.

Hide Answer

Suggested Answer:



by J108 at *March 18, 2025, 12:29 p.m.*

Comments

starlord45 Highly Voted 8 months ago

In my opinion the following solution is the best:
1. Create a sensitivity label.
2. Create an auto-labeling policy.
3. Wait 24 hours and then turn on the policy.

Create a retention label. -> Has nothing to do with information protection.
Create a sensitive info type. -> Not needed because for credit cards, there is a built-in one.

To be honest, the Wait 24 hours and then turn on the policy, does not sound that good for me.
But the other ones are even worse... .

upvoted 22 times

AttackOnMinion 6 months, 2 weeks ago

believe the 24 hour aims to let the simulation mode complete

upvoted 2 times

Tomrr Most Recent 1 month ago

There is no retention policy listed for site1. States All M365 user documents must be retained for 1 year.

1. retention label
2. sensitivity label
3. auto-labeling policy

upvoted 2 times

Eltooth 2 months, 1 week ago

1. Create a sensitivity label. 2. Create an auto-labeling policy. 3. Wait 24 hours and then turn on the policy.

upvoted 2 times

dmoorthy 3 months ago

1. Create a sensitivity label.
2. Create an auto-labeling policy.
3. Wait 24 hours and then turn on the policy.

upvoted 1 times

phatboi 4 months, 4 weeks ago

the question said all the technical requirements for site 1 should be met. Site one contains credit data hence an SIT needs to be defined, a label created and an auto labelling applied. You may ask but there is an inbuild SIT for credit card, that is fine but you have to customize it because it might not be suitable to match your requirement.

upvoted 1 times

Jdr379 5 months, 2 weeks ago

1. Create a sensitivity label
2. Create an auto-labeling policy
3. Wait 24 hours and then turn on the policy

upvoted 1 times

KrisDeb 7 months ago

1. Create a sensitivity label
2. Create an auto-labelling policy
3. Wait 24 hours and then turn on the policy

Create a retention label - N/A
Create a sensitive info type - No need, already built-in

upvoted 3 times

Fiqri 7 months, 3 weeks ago

You need to meet the technical requirements for the Site1 documents.

Doesn't that means all documents/data should be retained for 1 year? so we need to configure retention policy too, waiting 24 hours doesn't make any sense because that doesn't mean we wait 24 hours after we turned on the policy, it says wait 24 hours then turn on policy. The given answer is correct for me

upvoted 3 times

Fiqri 7 months, 3 weeks ago

i mean
1. retention label
2. sensitivity label
3. auto-labeling policy

upvoted 5 times

J108 8 months, 4 weeks ago

Create Sensitivity Label
Create an Autolabeling Policy
Wait 24 hours and then rurn on the policy

"Create a sensitive info type" isn't needed because credit card numbers are a built-in sensitive info type.

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 1 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 1
Topic #: 2
[All SC-401 Questions]

HOTSPOT -

Case Study -

Instructions -
This is a case study. Case studies are not timed separately from other exam sections. You can use as much exam time as you would like to complete each case study. However, there might be additional case studies or other exam sections. Manage your time to ensure that you can complete all the exam sections in the time provided. Pay attention to the Exam Progress at the top of the screen so you have sufficient time to complete any exam sections that follow this case study.
To answer the case study questions, you will need to reference information that is provided in the case. Case studies and associated questions might contain exhibits or other resources that provide more information about the scenario described in the case. Information provided in an individual question does not apply to the other questions in the case study.
A Review Screen will appear at the end of this case study. From the Review Screen, you can review and change your answers before you move to the next exam section. After you leave this case study, you will NOT be able to return to it.

To start the case study -
To display the first question in this case study, select the "Next" button. To the left of the question, a menu provides links to information such as business requirements, the existing environment, and problem statements. Please read through all this information before answering any questions. When you are ready to answer a question, select the "Question" button to return to the question.

Overview -
Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.

Existing Environment -

Microsoft 365 Environment -
Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

Users store data in the following locations:

SharePoint sites -

OneDrive accounts -

Exchange email -

Exchange public folders -

Teams chats -

Teams channel messages -
When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

SharePoint Online Environment -
Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.
Site2 contains the files shown in the following table.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.
Site4 has the following two retention policies applied:

Name: Site4RetentionPolicy1 -
Locations to apply the policy: Site4
Delete items older than: 2 years
Delete content based on: When items were created

Name: Site4RetentionPolicy2 -
Locations to apply the policy: Site4
Retain items for a specific period: 4 years
Start the retention period based on: When items were created
At the end of the retention period: Do nothing

Problem Statements -
Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

Requirements -

Planned Changes -
Contoso plans to create the following data loss prevention (DLP) policy:

Name: DLPpolicy1 -
Locations to apply the policy: Site2
Conditions:
Content contains any of these sensitive info types: SWIFT Code

Instance count: 2 to any -
Actions: Restrict access to the content

Technical Requirements -

Contoso must meet the following technical requirements:

All administrative users must be able to review DLP reports.

Whenever possible, the principle of least privilege must be used.

For all users, all Microsoft 365 data must be retained for at least one year.

Confidential documents must be detected and protected by using Microsoft 365.

Site1 documents that include credit card numbers must be labeled automatically.

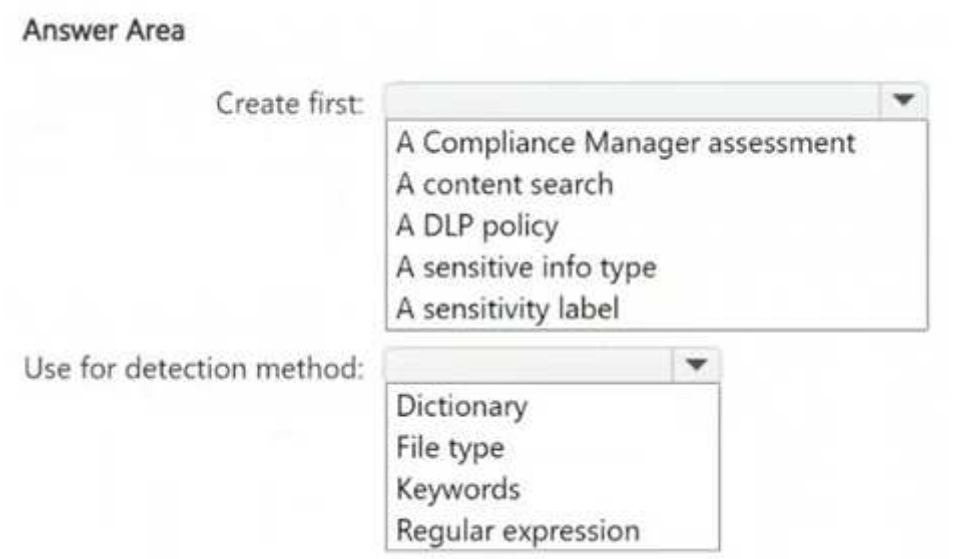
All administrative users must be able to create Microsoft 365 sensitivity labels.

After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.

You need to meet the technical requirements for the confidential documents.

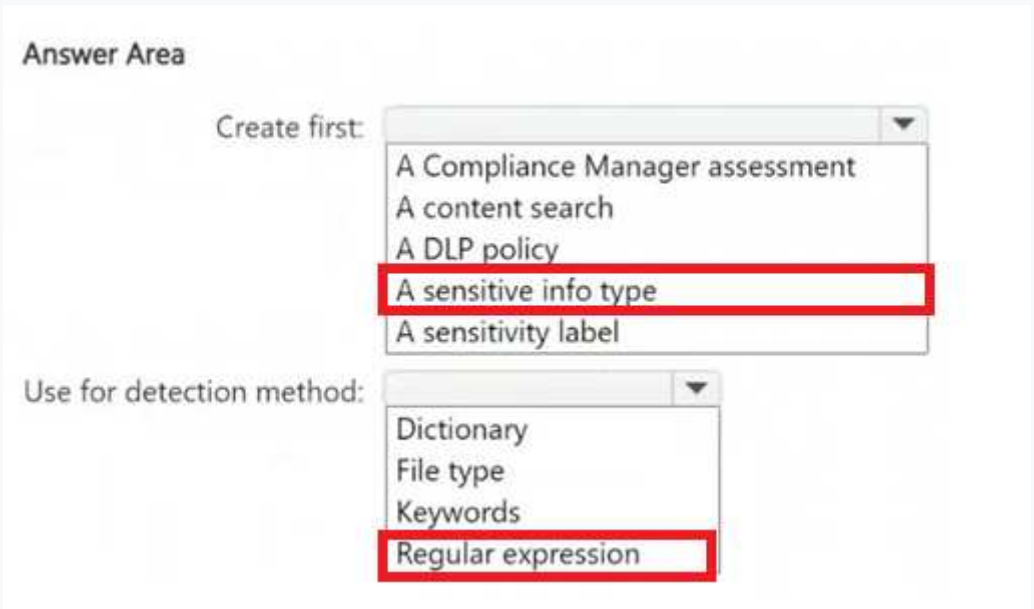
What should you create first, and what should you use for the detection method? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Hide Answer

Suggested Answer:



by Koenst at *June 16, 2025, 1:49 p.m.*

Comments

Eltooth 2 months, 2 weeks ago

SIT
RegEx

upvoted 2 times

> **Eltooth** 2 months, 1 week ago
>
> "When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential."
>
> upvoted 2 times

Koenst 5 months, 4 weeks ago

a default sit for creditcard already exist so i think it it create a sensitity label first

upvoted 3 times

> **zied01** 4 months, 3 weeks ago
>
> docs that are confidential are with digit codes 999 : it require a custom SIT and regex
>
> upvoted 7 times

Gtc_ 3 months, 2 weeks ago

Creating a SIT alone doesn't auto label. Need to create a sensitivity label first and then apply the reg ex for credit card.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 2 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 2
Topic #: 1
[All SC-401 Questions]

Case Study -

Instructions -
This is a case study. Case studies are not timed separately from other exam sections. You can use as much exam time as you would like to complete each case study. However, there might be additional case studies or other exam sections. Manage your time to ensure that you can complete all the exam sections in the time provided. Pay attention to the Exam Progress at the top of the screen so you have sufficient time to complete any exam sections that follow this case study.
To answer the case study questions, you will need to reference information that is provided in the case. Case studies and associated questions might contain exhibits or other resources that provide more information about the scenario described in the case. Information provided in an individual question does not apply to the other questions in the case study.
A Review Screen will appear at the end of this case study. From the Review Screen, you can review and change your answers before you move to the next exam section. After you leave this case study, you will NOT be able to return to it.

To start the case study -
To display the first question in this case study, select the "Next" button. To the left of the question, a menu provides links to information such as business requirements, the existing environment, and problem statements. Please read through all this information before answering any questions. When you are ready to answer a question, select the "Question" button to return to the question.

Overview -
Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.

Existing Environment -

Microsoft 365 Environment -
Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

Users store data in the following locations:

SharePoint sites -

OneDrive accounts -

Exchange email -

Exchange public folders -

Teams chats -

Teams channel messages -
When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

SharePoint Online Environment -
Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.
Site2 contains the files shown in the following table.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.
Site4 has the following two retention policies applied:

Name: Site4RetentionPolicy1 -
Locations to apply the policy: Site4
Delete items older than: 2 years
Delete content based on: When items were created

Name: Site4RetentionPolicy2 -
Locations to apply the policy: Site4
Retain items for a specific period: 4 years
Start the retention period based on: When items were created
At the end of the retention period: Do nothing

Problem Statements -
Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

Requirements -

Planned Changes -
Contoso plans to create the following data loss prevention (DLP) policy:

Name: DLPpolicy1 -
Locations to apply the policy: Site2
Conditions:
Content contains any of these sensitive info types: SWIFT Code

Instance count: 2 to any -
Actions: Restrict access to the content

Technical Requirements -

Contoso must meet the following technical requirements:
All administrative users must be able to review DLP reports.
Whenever possible, the principle of least privilege must be used.
For all users, all Microsoft 365 data must be retained for at least one year.
Confidential documents must be detected and protected by using Microsoft 365.
Site1 documents that include credit card numbers must be labeled automatically.
All administrative users must be able to create Microsoft 365 sensitivity labels.
After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.
You need to meet the technical requirements for the creation of the sensitivity labels.
To which user or users must you assign the Sensitivity Label Administrator role?

A. Admin1 only
B. Admin1 and Admin4 only Most Voted
C. Admin1 and Admin5 only
D. Admin1, Admin2, and Admin3 only
E. Admin1, Admin2, Admin4, and Admin5 only

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (70%) E (30%)

by Jo696 at *April 1, 2025, 1:57 a.m.*

Comments

Weishaupt Highly Voted 6 months, 3 weeks ago

Selected Answer: B

Right answer is B:
https://learn.microsoft.com/en-us/purview/get-started-with-sensitivity-labels

Permissions required to create and manage sensitivity labels:

"Another option is to add users to the Compliance Data Administrator, Compliance Administrator, or Security Administrator role group."

upvoted 11 times

f2b34cb Most Recent 1 month ago

Selected Answer: E

To create sensitivity labels, you need an administrative role like Global Administrator, Compliance Administrator, or one of the Information Protection roles (Information Protection, Information Protection Admin, Information Protection Analyst, Information Protection Investigator, or Information Protection Reader). The Security Administrator role also includes permissions to manage sensitivity labels.

upvoted 1 times

265cb32 1 month ago

Selected Answer: E

The only administrator from the list that has the ability to create labels is the "Compliance Administrator", the others do not have the rights to create labels, not even the "Compliance Data Administrator" because it's more focused on data access and compliance.
Therefore the answer is E.

upvoted 2 times

dmoorthy 3 months ago

Selected Answer: B

Requirement :All administrative users must be able to create Microsoft 365 sensitivity labels.
Question is "To which user or users must you assign the Sensitivity Label
Administrator role"

Answer: By default Compliance Data Administrator, Compliance Administrator, or Security Administrator can create sensitivity labels.

So add Sensitivity Label Administrator role only to Admin1: Global reader and Admin4: security operator.

upvoted 1 times

deeptha92 3 months, 2 weeks ago

Selected Answer: B

Alternatively to using the default role groups, you can create a new role group and add the Sensitivity Label Administrator role to this group. For a read-only role, use Sensitivity Label Reader.

Another option is to add users to the Compliance Data Administrator, Compliance Administrator, or Security Administrator role group.

upvoted 1 times

laykay4me 3 months, 3 weeks ago

Selected Answer: E

Since the requirement is for all administrators to be able to create a sensitivity information label, and out of all the administrators, only the compliance administrator has that permission without the assignment of the sensitivity label administrator role. Then the other administrator will need the role assigned to them first before they can create the label.

upvoted 1 times

laykay4me 3 months, 2 weeks ago

From further studies, I realise aside the global reader and security operators roles, every other roles can create sensitivity label. Hence the correct answer is B and not E as I initially went for.

upvoted 1 times

Jdr379 5 months, 2 weeks ago

Selected Answer: B

Agree with B

upvoted 2 times

examtopicssc401 6 months ago

Selected Answer: B

Admin1 (Global Reader) and Admin4 (Security Operator) do not have permissions to create sensitivity labels, so they would need the Sensitivity Label Administrator role assigned if you want all admins to have this capability, as required by the scenario.

upvoted 2 times

Jacobddu 6 months, 1 week ago

Selected Answer: B

Admin2, 3, 5 all have the permission by default.

upvoted 2 times

rodscherdead 7 months, 1 week ago

Selected Answer: B

Right answer is B:
https://learn.microsoft.com/en-us/purview/get-started-with-sensitivity-labels

Permissions required to create and manage sensitivity labels:

"Another option is to add users to the Compliance Data Administrator, Compliance Administrator, or Security Administrator role group."

upvoted 3 times

starlord45 8 months ago

Selected Answer: E

For me Answer E fits the most.

A Global Reader only can view only settings and can not create labels.

Compliance Data Administrator can keep track of your organization's data across Microsoft 365, make sure it's protected, and get insights into any issues to help mitigate risks.

Compliance Administrator can create sensitivity labels.

Security Operator can not create labels, has more rights in defender xdr than in purview.

Security Administrator, same as Security Operator. More rights in defender xdr, but can not create labels.

So answer E.
Admin1, Admin2, Admin4, and Admin5
should be right.

upvoted 2 times

JFROG 8 months, 1 week ago

Selected Answer: B

I agree with ETUs3r. https://learn.microsoft.com/en-us/entra/architecture/8-secure-access-sensitivity-labels

Permissions to create and manage sensitivity levels
Team members who need to create sensitivity labels require permissions to:

Microsoft 365 Defender portal,
Microsoft Purview compliance portal, or
Microsoft Purview compliance portal
By default, Global Administrators have access to admin centers and can provide access, without granting tenant Admin permissions. For this delegated limited admin access, add users to the following role groups:

Compliance Data Administrator,
Compliance Administrator, or
Security Administrator

upvoted 1 times

ETUs3r 8 months, 1 week ago

Selected Answer: B

Correct answer should be B.
https://learn.microsoft.com/en-us/defender-office-365/scc-permissions

upvoted 3 times

RoMoo 8 months, 2 weeks ago

Selected Answer: E

Admin3 (Compliance Administrator) already has this permission through their existing role.
The users who need the "Sensitivity Label Administrator" role assigned are those who do not already have the permission via another role. These are Admin1, Admin2, Admin4, and Admin5.

upvoted 3 times

Jo696 8 months, 2 weeks ago

Selected Answer: E

Only admin 3, the compliance administrator, can create sensitivity labels

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 3 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 3
Topic #: 1
[All SC-401 Questions]

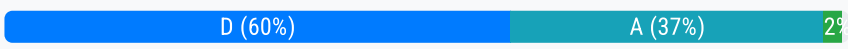
You have a Microsoft 365 E5 subscription that contains a Microsoft Teams channel named Channel1. Channel1 contains research and development documents.
You plan to implement Microsoft 365 Copilot for the subscription.
You need to prevent the contents of files stored in Channel1 from being included in answers generated by Copilot and shown to unauthorized users.
What should you use?

A. data loss prevention (DLP)
B. Microsoft Purview insider risk management
C. Microsoft Purview Information Barriers (IBs)
D. sensitivity labels Most Voted

Hide Answer

Suggested Answer: *D*

Community vote distribution



by Skippy1969 at *March 27, 2025, 9:41 p.m.*

Comments

dmoorthy Highly Voted 3 months ago

Selected Answer: D
Sensitivity Labesl.
Copilot respects sensitivity labels and will not surface protected content to users who are not authorized.
upvoted 6 times

265cb32 Most Recent 3 months, 1 week ago

Selected Answer: D
D because you can disable the "copy and extract content" option from the label configuration, however, you can also create a DLP policy that will prevent copilot from processing content that has a specific sensitivity label applied to documents (this is a more easier and fast option to apply lately).
upvoted 2 times

deeptha92 3 months, 2 weeks ago

Selected Answer: D

I would go with D on this one.

upvoted 1 times

laykay4me 3 months, 2 weeks ago

Selected Answer: A

I will go for A because we are protecting content of a file and not just a document. Hence, sensitivity label would have to be applied to each documents individually even when you have to use auto labelling. The best option is DLP

upvoted 1 times

Suranka 3 months, 3 weeks ago

Selected Answer: D

The right control is Microsoft Purview Information Protection (sensitivity labels with scoped permissions

upvoted 1 times

gabbinu 3 months, 3 weeks ago

Selected Answer: D

Answer is D.
you must apply sensitivity labels that restrict access to authorized users only.
if an unauthorized user tries to query Copilot, Copilot can't read the file → it won't use that content in its responses.

upvoted 1 times

8d1e8fe 3 months, 3 weeks ago

Selected Answer: D

The sensitivity label is the basis for the DLP setting to begin with. Copilot however DOES respect a DLP policy based on that label. Typical Microsoft question not entirely MECE.

upvoted 1 times

DrArjunReddy 4 months, 2 weeks ago

Selected Answer: D

Answer should be D. Can do DLP without sensitivity labels and even with out DLP, removing encryption on the sensitivity label itself should prevent unauthorized access.

upvoted 1 times

Flacky_Penguin32 4 months, 3 weeks ago

Selected Answer: A

I used this control at work; its def A. It was in private preview for a while and now is available for DLP polices.

upvoted 1 times

zied01 4 months, 3 weeks ago

Selected Answer: D

the dlp policy is based on the senstive labels , so the answer is D

upvoted 1 times

phatboi 4 months, 4 weeks ago

o minimize the risk of General Data Protection Regulation (GDPR) data being included in Microsoft 365 Copilot summaries and also exclude private information from summaries. They plan to create a DLP policy that uses the Microsoft 365 Copilot policy location with the Content contains > Sensitivity labels condition to exclude items that have the Personal sensitivity label from being processed in the response summary and also to exclude items that have the Highly Confidential sensitivity label from being processed in the response summary.

upvoted 1 times

Jdr379 5 months, 2 weeks ago

Selected Answer: D

Agree with D

upvoted 1 times

2ff2acc 5 months, 4 weeks ago

Selected Answer: D

Answer D
Why the other options are incorrect:
A. Data Loss Prevention (DLP): DLP helps prevent data exfiltration (such as emailing sensitive data), but it does not control what Copilot can access or generate in its responses.

B. Insider Risk Management: This is used to detect and respond to risky user behavior (like data leaks or misuse), but it does not prevent Copilot from accessing data.

C. Information Barriers (IBs): IBs prevent communication and collaboration between certain groups, but they don't apply to Copilot's data processing directly unless configured very strictly—and still wouldn't control Copilot's access to a specific channel's data as precisely as sensitivity labels.

upvoted 1 times

examtopicssc401 6 months ago

Selected Answer: D

Sensitivity labels (D): You can apply sensitivity labels to documents in Channel1 (such as "Top Secret" or "Highly Confidential"). Sensitivity labels can be configured to block connected experiences like Copilot from processing the content of labeled files, effectively preventing Copilot from including that content in its answers. This is done either through advanced settings (like BlockContentAnalysisServices) or by applying encryption with user-defined permissions

upvoted 1 times

aBCCERT 6 months ago

Selected Answer: A

While sensitivity labels (option D) can classify and protect documents, they do not directly control whether Copilot can access or reference them in responses. Microsoft Purview

upvoted 3 times

examtopicssc401 6 months, 1 week ago

Selected Answer: D

Sensitivity labels allow you to:

Classify and protect content (e.g., "Confidential – R&D").
Restrict access to the labeled files using encryption and permissions.
Copilot respects label-based access control, meaning it won't include content from protected files in responses unless the user has access.

upvoted 2 times

mhmyz 6 months, 2 weeks ago

Selected Answer: D

D. Sensitivity labels
How Microsoft 365 Copilot works with sensitivity labels and encryption
https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-architecture-data-protection-auditing#how-microsoft-365-copilot-works-with-sensitivity-labels-and-encryption

upvoted 1 times

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 4 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 4

Topic #: 1

[All SC-401 Questions]

DRAG DROP -

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.

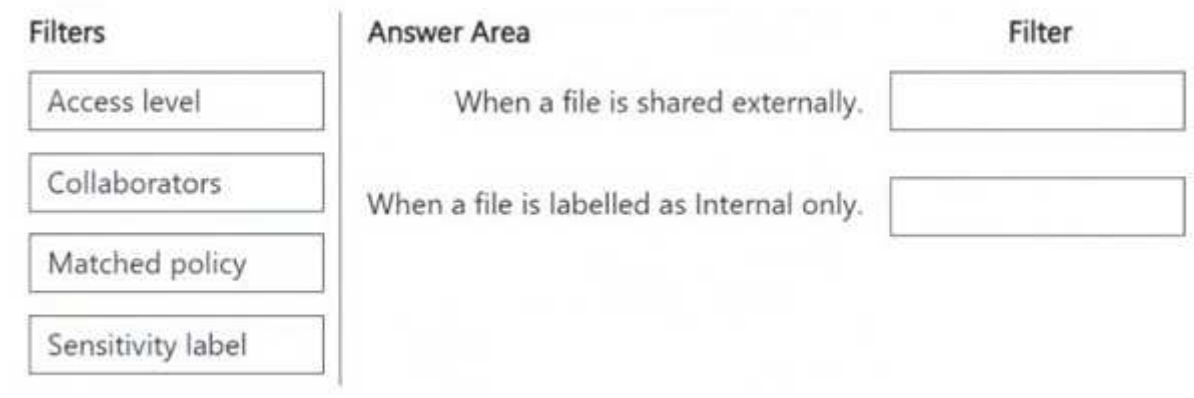
You plan to deploy a Defender for Cloud Apps file policy that will be triggered when the following conditions are met:

A file is shared externally.

A file is labeled as internal only.

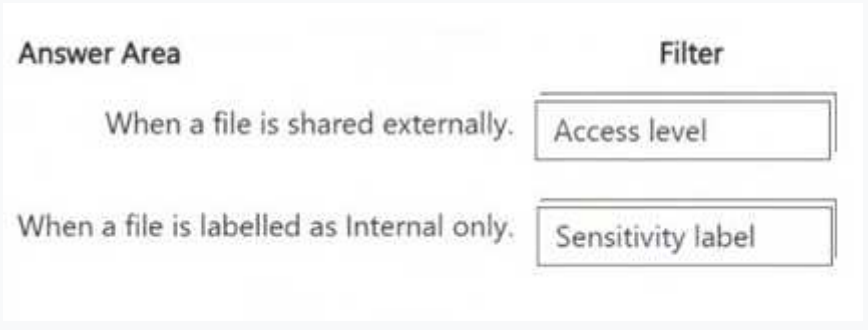
Which filter should you use for each condition? To answer, drag the appropriate filters to the correct conditions. Each filter may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Hide Answer

Suggested Answer:



by starlord45 at *April 17, 2025, 8:14 a.m.*

Comments

Fiqri Highly Voted 7 months, 3 weeks ago

the answer is correct.

upvoted 7 times

dmoorthy Most Recent 3 months ago

Answer is correct.
upvoted 1 times

deeptha92 3 months, 2 weeks ago
Given answer is correct.
upvoted 1 times

RamyKetata 7 months, 1 week ago
A file is shared externally → Use "Access level"

This filter allows you to set conditions for files that are shared externally versus internally.

You should configure it to detect files that have an external sharing status.

A file is labeled as internal only → Use "Sensitivity label"

This filter enables Defender for Cloud Apps to recognize files with specific sensitivity labels.

Select the "Internal Only" label to trigger the policy when such files are involved.
upvoted 3 times

starlord45 7 months, 4 weeks ago
Seems right.

When a file is shared externally [Access level].
The following access levels are possible:
Public (Internet), Public, External, Internal, Private.

When a file is labelled as internal only. [Sensivity label]
Filter should look like this:
Sensitivity label - Microsoft Information Protection equals Internal-Label.
upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 5 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 5
Topic #: 1
[All SC-401 Questions]

HOTSPOT -

You have a Microsoft 365 E5 subscription that contains three DOCX files named File1, File2, and File3.

You create the sensitivity labels shown in the following table.

Name	Permission	Apply content marking
Label1	Any authenticated users: Viewer	Disabled
Label2	*None*	Enabled

You apply the labels to the files as shown in the following table.

File	Label
File1	*None*
File2	Label1
File3	Label2

You ask Microsoft 365 Copilot to summarize the files, and you receive the results shown in the following table.

Name	Based on content of
Summary1	File1, File3
Summary2	File2
Summary3	File1, File2, File3

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

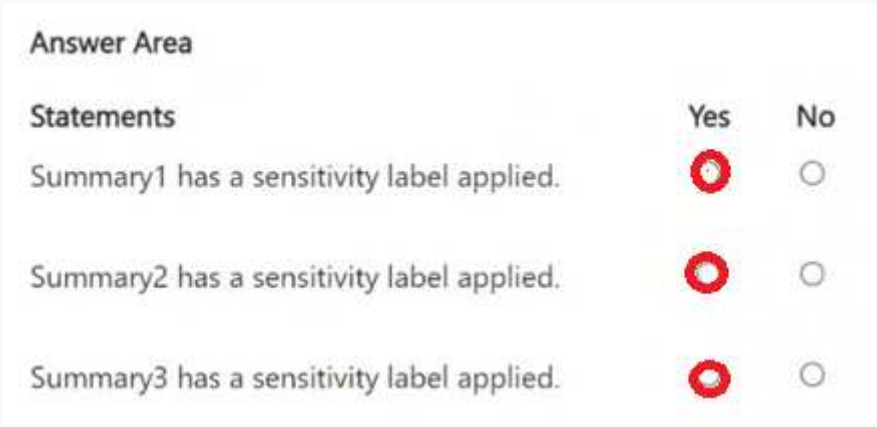
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Summary1 has a sensitivity label applied.	○	○
Summary2 has a sensitivity label applied.	○	○
Summary3 has a sensitivity label applied.	○	○

Hide Answer

Suggested Answer:



by starlord45 at *April 17, 2025, 8:24 a.m.*

Comments

starlord45 Highly Voted 7 months, 4 weeks ago

Every Summary should have a label assigned, because Copilot can work with the applied labels and always inherits the label with the highest priority.

https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-architecture-data-protection-auditing

Therefore, because each Summary has at least one labeled file, every summary has a label assigned.

upvoted 9 times

Fiqri 7 months, 3 weeks ago

correct

upvoted 2 times

brugmany Most Recent 2 weeks, 2 days ago

I was initially confused, but I figured it out: Copilot summaries always include a sensitivity label, either inherited from the source file or automatically applied by policy.

upvoted 1 times

Ender3 2 months ago

While I am going along with the triple Yes answer, I believe Summary2 should fail to summarize File2 because Label1 is applied to it, restricting access to Viewer only, which does not include EXTRACT permission. I am staying with Yes on Summary2 because allegedly a summary was created based on File2.

upvoted 2 times

dmoorthy 3 months ago

Yes, yes, yes

upvoted 1 times

gabbinu 3 months, 2 weeks ago

Yes, Yes, Yes
When Microsoft 365 Copilot generates a new file (e.g. a summary), if the source content has sensitivity labels, the summary inherits the highest priority label from its sources.

upvoted 1 times

javifedz 6 months, 2 weeks ago

No, Yes, Yes

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 6 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 6
Topic #: 1
[All SC-401 Questions]

You have a Microsoft 365 E5 subscription.
You need to create a sensitivity label named Label1. The solution must ensure that users can use Microsoft 365 Copilot to summarize files that have Label1 applied.
Which permission should you select for Label1?

A. Export content(EXPORT)
B. Copy and extract content(EXTRACT) Most Voted
C. Edit content(DOCEDIT)
D. View rights(VIEW)

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (73%) D (21%) 6%

by RoMoo at *April 2, 2025, 11:46 p.m.*

Comments

Fiqri Highly Voted 7 months, 3 weeks ago

Selected Answer: B

according to this article: https://learn.microsoft.com/en-us/purview/ai-microsoft-purview-considerations

If content grants a user VIEW usage rights but not EXTRACT:
Copilot won't summarize this content but can reference it with a link so the user can then open and view the content outside Copilot.

So the answer is B.

upvoted 10 times

javifedz Highly Voted 6 months, 2 weeks ago

Selected Answer: B

Copy and extract content (EXTRACT)

upvoted 6 times

dmoorthy Most Recent 3 months ago

Selected Answer: B

Copy and extract content (EXTRACT)

upvoted 1 times

gabbinu 3 months, 3 weeks ago

Selected Answer: B

Answer is B

https://learn.microsoft.com/en-us/purview/sensitivity-labels
"If the labels applied encryption from Microsoft Purview Information Protection, Copilot and agents check the usage rights for the user. Only if the user is granted permissions to copy (the EXTRACT usage right) from an item, is data from that item returned by Copilot or agents."

upvoted 2 times

GregJ123456 5 months, 2 weeks ago

Selected Answer: C

Tried setting up files with all the below sensitivty labels. Shared it with different user. Guess what worked for the other user. The one whcih had C on it.
But for the creator of this file, it worked on B.
Hence I will select C as this is required for Co-pilot to work

upvoted 1 times

GregJ123456 5 months, 2 weeks ago

Selected Answer: C

Tried setting up files with all the below sensitivty labels. Shared it with different user. Guess what worked for the other user. The one whcih had C on it.
But for the creator of this file, it worked on B.
Hence I will select C as this is required for Co-pilot to work

upvoted 1 times

tuantmb 6 months ago

Selected Answer: B

EXTRACT allows services like Copilot to read and process the content for summarization, insights, and other AI-powered features.

upvoted 1 times

tuantmb 6 months ago

Selected Answer: B

Same as previous users, copilot needs EXTRACT permission to process data (VIEW permission only allow use resource as reference)

upvoted 1 times

Jarem 6 months, 2 weeks ago

Selected Answer: B

In the Microsoft Purview portal, the EXTRACT usage right is displayed as Copy and extract content(EXTRACT). For example, the default permission level selected is Editor, where you see Copy and extract content(EXTRACT) is included. As a result, content protected with this encryption configuration can be returned by Copilot and agents https://learn.microsoft.com/en-us/purview/ai-microsoft-purview-considerations#copilot-honors-existing-protection-with-the-extract-usage-right

upvoted 1 times

TheMCT 7 months, 1 week ago

Selected Answer: D

To ensure that Microsoft 365 Copilot can summarize files with a sensitivity label applied, the label must grant Copilot the ability to read and process the content.

upvoted 2 times

rodscherdead 7 months, 3 weeks ago

Selected Answer: D

https://learn.microsoft.com/en-us/purview/ai-microsoft-purview-considerations

If content grants a user VIEW usage rights but not EXTRACT:
- When a user has this content open in an app, they won't be able to use Copilot.
- Copilot won't summarize this content but can reference it with a link so the user can then open and view the content outside Copilot.

When...open...in...an...app -> THIS content won´t summarize by Copilot
So I go with D

upvoted 3 times

starlord45 7 months, 4 weeks ago

Selected Answer: D

I consider D View rights (VIEW) as right.

Because a summary can be done from a user when he can view the content.
so open document and ask for a summary.
Common name: Copy

Encoding in policy: EXTRACT Enables options to copy data (including screen captures) from the document into the same or another document.

In some applications, it also allows the whole document to be saved in unprotected form.

Extract is more for reports and new documents generated on the source file.
But for a summary this is not needed.

https://learn.microsoft.com/en-us/azure/information-protection/configure-usage-rights

upvoted 1 times

JFROG 8 months ago

Selected Answer: B

I am going for B. Check https://learn.microsoft.com/en-us/purview/ai-microsoft-purview-considerations

If content grants a user VIEW usage rights but not EXTRACT:

When a user has this content open in an app, they won't be able to use Copilot.
Copilot won't summarize this content but can reference it with a link so the user can then open and view the content outside Copilot.

upvoted 2 times

RoMoo 8 months, 2 weeks ago

Selected Answer: D

VIEW is the minimum necessary permission for this specific task.

upvoted 1 times

EXAMTOPICS

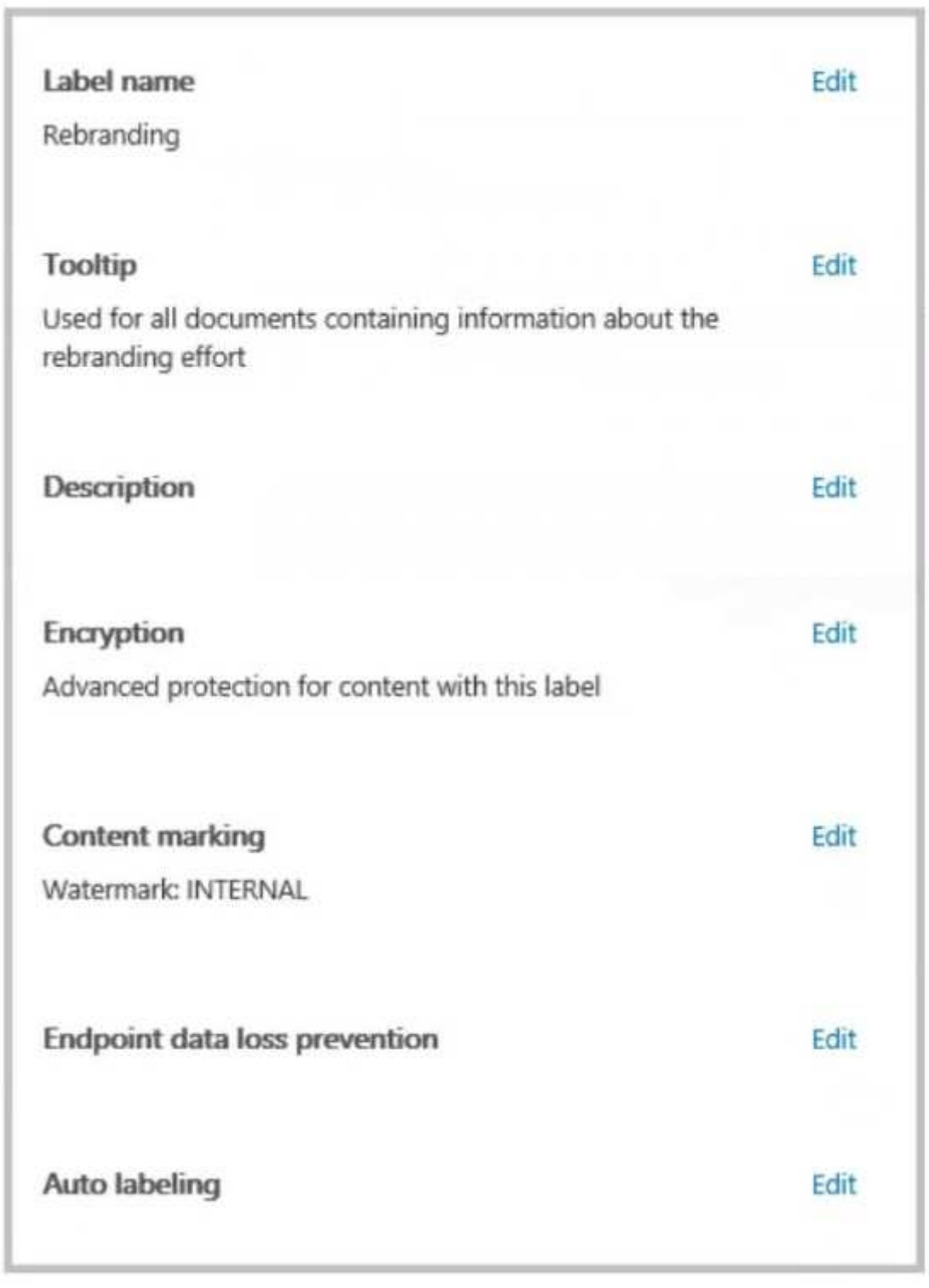
Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 7 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 7
Topic #: 1
[All SC-401 Questions]

HOTSPOT -
You have a Microsoft 365 sensitivity label that is published to all the users in your Microsoft Entra tenant as shown in the following exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
All the documents stored on each user's computer will include a watermark automatically.	○	○
If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL".	○	○
The sensitivity label can be applied only to documents that contain the word rebranding.	○	○

Hide Answer

Suggested Answer:

Answer Area

Statements	Yes	No
All the documents stored on each user's computer will include a watermark automatically.	○	●
If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL".	○	●
The sensitivity label can be applied only to documents that contain the word rebranding.	○	●

by starlord45 at *April 17, 2025, 9:27 a.m.*

Comments

dmoorthy 3 months ago

The given answer is Correct, No, No, No.

upvoted 2 times

AttackOnMinion 6 months, 2 weeks ago

NONONO
Mark the content when you use Office apps, by adding watermarks, headers, or footers to email, meeting invites, or documents that have the label applied. Watermarks can be applied to documents and Loop component and pages, but not email or meeting invites. Example header and watermark
https://learn.microsoft.com/en-us/purview/ai-microsoft-purview-considerations

upvoted 3 times

sesav4742 6 months, 4 weeks ago

The given answer is Correct, No, No, No.

upvoted 3 times

TheMCT 7 months, 1 week ago

The given answer is Correct, No, No, No.
The label applies a watermark, not a header. A watermark typically appears diagonally across the page, not in the header section.

upvoted 2 times

Fiqri 7 months, 3 weeks ago

NO, YES, NO.

upvoted 2 times

RamyKetata 7 months, 1 week ago

A watermark labeled "INTERNAL" typically appears as a faint text or image overlaid on each page of a document, often in the background.
So: NO,NO,NO

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 8 DISCUSSION

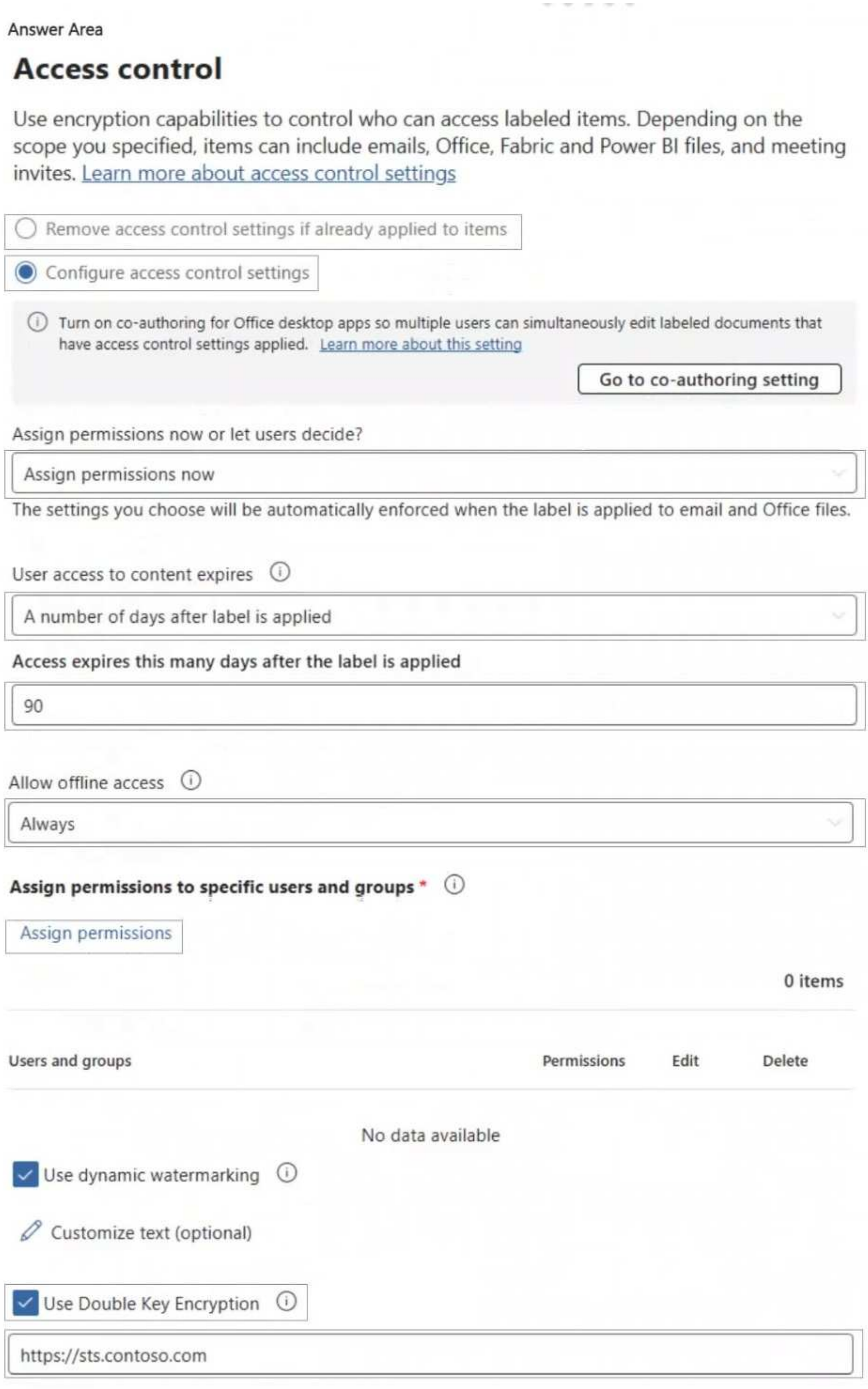
Actual exam question from Microsoft's SC-401
Question #: 8
Topic #: 1
[All SC-401 Questions]

HOTSPOT -
You have a Microsoft 365 E5 tenant that contains a sensitivity label named label1.
You plan to enable co-authoring for encrypted files.
You need to ensure that files that have label1 applied support co-authoring.

Which two settings should you modify? To answer, select the settings in the answer area.

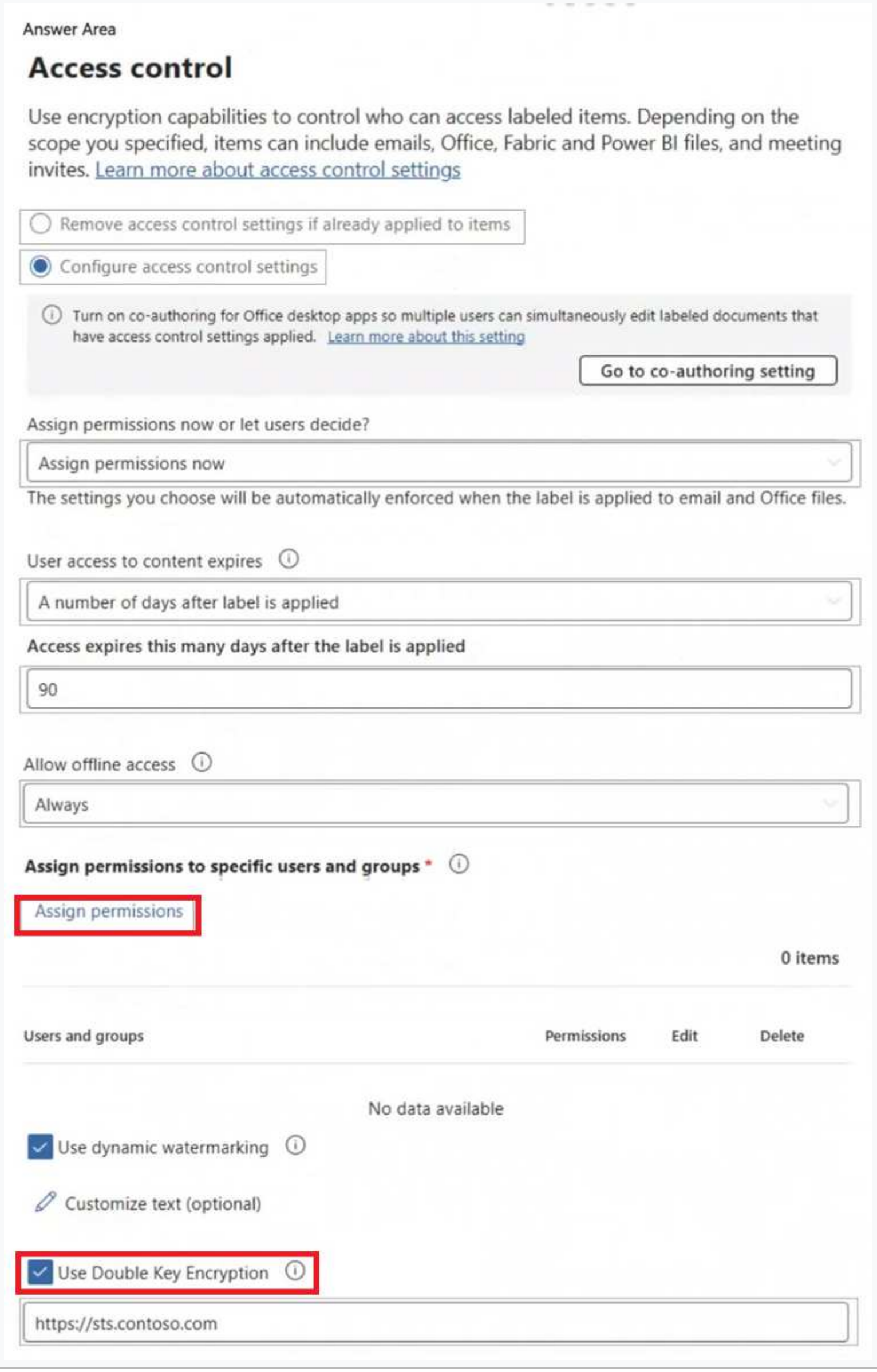
NOTE: Each correct selection is worth one point.

Answer Area


Access control
Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. Learn more about access control settings
Remove access control settings if already applied to items
Configure access control settings
Turn on co-authoring for Office desktop apps so multiple users can simultaneously edit labeled documents that have access control settings applied. Learn more about this setting
Go to co-authoring setting
Assign permissions now or let users decide?
Assign permissions now
The settings you choose will be automatically enforced when the label is applied to email and Office files.
User access to content expires
A number of days after label is applied
Access expires this many days after the label is applied
90
Allow offline access
Always
Assign permissions to specific users and groups *
Assign permissions
0 items
Users and groups
Permissions
Edit
Delete
No data available
Use dynamic watermarking
Customize text (optional)
Use Double Key Encryption
https://sts.contoso.com

Hide Answer

Suggested Answer:


Answer Area
Access control
Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. Learn more about access control settings
Remove access control settings if already applied to items
Configure access control settings
Turn on co-authoring for Office desktop apps so multiple users can simultaneously edit labeled documents that have access control settings applied. Learn more about this setting
Go to co-authoring setting
Assign permissions now or let users decide?
Assign permissions now
The settings you choose will be automatically enforced when the label is applied to email and Office files.
User access to content expires
A number of days after label is applied
Access expires this many days after the label is applied
90
Allow offline access
Always
Assign permissions to specific users and groups *
Assign permissions
0 items
Users and groups
Permissions
Edit
Delete
No data available
Use dynamic watermarking
Customize text (optional)
Use Double Key Encryption
https://sts.contoso.com

by starlord45 at *April 17, 2025, 9:42 a.m.*

Comments

Newb007 Highly Voted 6 months, 4 weeks ago

https://learn.microsoft.com/en-us/purview/sensitivity-labels-coauthoring#limitations

User access to content expirers (not supported)
Double Key encryption (not supported)

upvoted 11 times

Ender3 Most Recent 2 months, 1 week ago

I kind of agree with the last 2 posters. And based on the article link by Newb007, perhaps the expected answer is "access expires" and "double key encryption" - makes sense.

However, I think "turn on co-authoring" is a third and valid part of the answer. Without it co-authoring is not possible. Thus, the exam question should have allowed for 3 correct responses, not just two.

Assign permissions is not relevant here because if you don't assign permissions now, you are letting users decide when they apply the label. This one is a red herring.

upvoted 1 times

Ender3 2 months ago

I take my comment about co-authoring back because the purpose of this question is to determine what is needed so that when co-authoring is enabled it will work.

upvoted 2 times

Nurob 3 months, 3 weeks ago

Both double key encryption and user access to content expiration settings can restrict the use of co-authoring and AutoSave functionalities. Specifically, if a sensitivity label is configured for double key encryption, co-authoring will not be supported. Similarly, if user access to content is set to expire when not set to “Never,” users will also face limitations in collaborating in real-time on those documents.

upvoted 2 times

gabbinu 3 months, 3 weeks ago

• Double Key Encryption (DKE) must be disabled to support co-authoring.
• Assign permissions - Users must be granted at least EDIT (DOCEDIT) rights to allow co-authoring.

upvoted 1 times

gabbinu 3 months, 2 weeks ago

Sorry, the two settings are:
- User access to content expires
- Double Key Encryption

https://learn.microsoft.com/en-us/purview/sensitivity-labels-coauthoring
Co-authoring and AutoSave aren't supported for Office documents that use the label encryption configuration User access to content expires when it's set to a value other than Never, or Double Key Encryption is configured.

upvoted 1 times

tuantmb 6 months ago

assign permission to user (you want to co-author) and remove DKE checked because enabled DKE cannot allow co-authoring

upvoted 1 times

rodscherdead 7 months, 3 weeks ago

AI say´s: No, co-authoring is not supported for files protected with Double Key Encryption (DKE).

upvoted 1 times

starlord45 7 months, 4 weeks ago

To be honest I do not really understand that question completly.
But I go for "Go to co-authoring setting" and enable that feature.
##
Co-authoring for files with sensitivity labels
This setting allows users in your organization to co-author in Office desktop documents that are encrypted by using sensitivity labels. To support this new capability, all users must have the latest Microsoft 365 Apps for enterprise and label metadata must be upgraded for all labeled documents that aren't encrypted.

https://learn.microsoft.com/en-us/purview/sensitivity-labels-coauthoring
##

And of course "Assign permissions" without this you can not click next.

I do not know why I should disable or enable Double Key Encryption (DKE)?
Because it is for encrypted files, and I do not see why this should not work with DKE.

upvoted 2 times

RamyKetata 7 months, 1 week ago

If you want to enable co-authoring for encrypted files, you should disable Double Key Encryption (DKE).

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 9 DISCUSSION

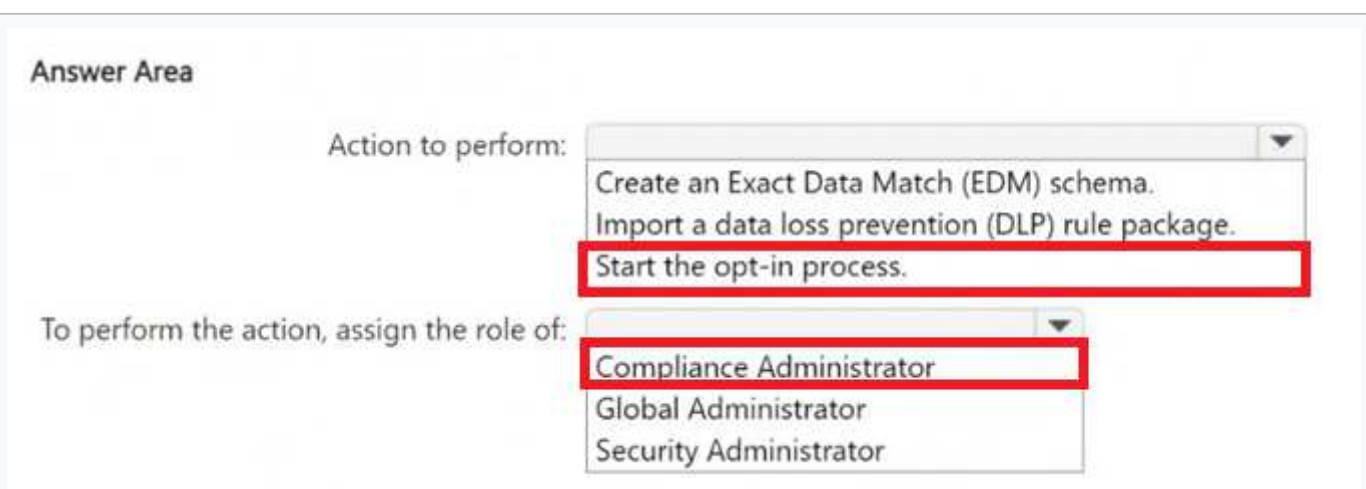
Actual exam question from Microsoft's SC-401
Question #: 9
Topic #: 1
[All SC-401 Questions]

HOTSPOT -
You have a new Microsoft 365 E5 tenant.
You need to create a custom trainable classifier that will detect product order forms. The solution must use the principle of least privilege.
What should you do first? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area
Action to perform:
Create an Exact Data Match (EDM) schema.
Import a data loss prevention (DLP) rule package.
Start the opt-in process.
To perform the action, assign the role of:
Compliance Administrator
Global Administrator
Security Administrator

Hide Answer

Suggested Answer:


Answer Area
Action to perform:
Create an Exact Data Match (EDM) schema.
Import a data loss prevention (DLP) rule package.
Start the opt-in process.
To perform the action, assign the role of:
Compliance Administrator
Global Administrator
Security Administrator

by pjn at *July 14, 2025, 1:42 p.m.*

Comments

dmoorthy 3 months ago
Answer is correct. If you are using the trainable classifier for the first time you will have to opt-in. You can validate the same by running the powershell command get-classifier
upvoted 1 times

gabbinu 3 months, 3 weeks ago

It should be an older question, you just go into the Purview portal and start creating classifiers — there's no opt-in step anymore.

upvoted 1 times

pjn 5 months ago

Start Opt-In and Global Admin at least according to Co-Pilot

upvoted 1 times

nuin01 3 weeks, 6 days ago

Start Opt-In and Global Admin Because "starting an opt-in process" often involves significant tenant-wide changes or enabling powerful features, it typically requires the highest level of authority.

upvoted 2 times

EXAMTOPICS

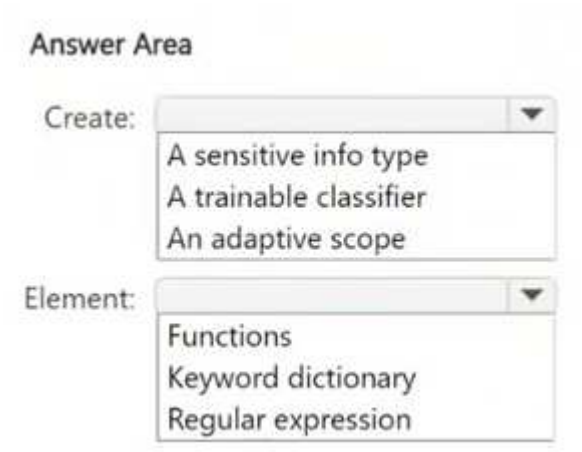
Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 10 DISCUSSION

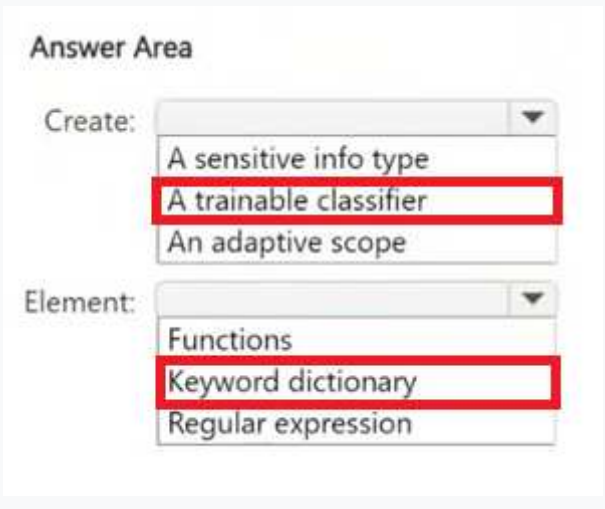
Actual exam question from Microsoft's SC-401
Question #: 10
Topic #: 1
[All SC-401 Questions]

HOTSPOT -
You have a Microsoft 365 E5 subscription.
You have a file named Customer.csv that contains a list of 1,000 customer names.
You plan to use Customer.csv to classify documents stored in a Microsoft SharePoint Online library.
What should you create in the Microsoft Purview portal, and which type of element should you select? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Hide Answer

Suggested Answer:



by geekygurl at *May 20, 2025, 1:09 a.m.*

Comments

geekygurl Highly Voted 6 months, 3 weeks ago

wrong, it should be Sensitive Info Type/ Keyword dictionary
upvoted 25 times

CuentaRM10 Highly Voted 6 months, 2 weeks ago
Should be SIT/Keyword
upvoted 10 times

dmoorthy Most Recent 3 months ago
Answer is a SIT(EDM based) and Keyword dictionary.
upvoted 3 times

Eltooth 3 months, 2 weeks ago
SIT and keyword dictionary.
upvoted 4 times

Suranka 3 months, 2 weeks ago
To classify documents in SharePoint Online using a list of customer names from a Customer.csv file, the correct approach in Microsoft Purview is:
Create: A sensitive info type
Custom Sensitive Information Types (SITs) allow you to define patterns that identify specific content, such as customer names.
Element: Keyword dictionary
upvoted 3 times

leprechaun 6 months, 1 week ago
SIT/Keyword is right
upvoted 4 times

58d4802 6 months, 2 weeks ago
More specifically, you would use an Exact Data Match (EDM) sensitive information type.
So correct answer is Sensitive Info Type/Keyword Dictionary
upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 11 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 11
Topic #: 1
[All SC-401 Questions]

You have a Microsoft 365 E5 subscription.
You need to enable support for sensitivity labels in Microsoft SharePoint Online.
What should you use?

A. the Microsoft Purview portal Most Voted
B. the Microsoft Entra admin center
C. the SharePoint admin center
D. the Microsoft 365 admin center

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (100%)

by N44 at *March 21, 2025, 10:47 a.m.*

Comments

N44 Highly Voted 8 months, 3 weeks ago

Selected Answer: A

A - This is turned on in Purview
https://learn.microsoft.com/en-us/purview/sensitivity-labels-sharepoint-onedrive-files

upvoted 6 times

dmoorthy Most Recent 3 months ago

Selected Answer: A

Either Purview portal or powershell Set-SPOTenant -EnableAIPIntegration $true

upvoted 1 times

Eltooth 3 months, 2 weeks ago

Selected Answer: A

A is correct answer. Purview Portal.

upvoted 1 times

CuentaRM10 6 months, 2 weeks ago

Selected Answer: A

The answer is correct

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 12 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 12
Topic #: 1
[All SC-401 Questions]

You have a Microsoft 365 subscription.
You need to customize encrypted email for the subscription. The solution must meet the following requirements.
Ensure that when an encrypted email is sent, the email includes the company logo.
Minimize administrative effort.
Which PowerShell cmdlet should you run?

A. Set-IRMConfiguration
B. Set-OMEConfiguration Most Voted
C. Set-RMSTemplate
D. New-OMEConfiguration

Hide Answer

Suggested Answer: *B*

Community vote distribution
B (100%)

by ETUs3r at *April 4, 2025, 12:35 a.m.*

Comments

dmoorthy 3 months ago
Selected Answer: B
B is correct answer: Set-OMEConfiguration
upvoted 1 times

Eltooth 3 months, 2 weeks ago
Selected Answer: B
B is correct answer: Set-OMEConfiguration
upvoted 1 times

CuentaRM10 6 months, 2 weeks ago
Selected Answer: B
Correct
https://learn.microsoft.com/en-us/powershell/module/exchange/set-omeconfiguration?view=exchange-ps

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 13 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 13
Topic #: 1
[All SC-401 Questions]

You have a Microsoft 365 E5 subscription.
You need to ensure that encrypted email messages sent to an external recipient can be revoked or will expire within seven days.
What should you configure first?

A. a custom branding template Most Voted
B. a mail flow rule
C. a sensitivity label
D. a Conditional Access policy

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (74%) C (16%) 10%

by f5831d6 at *March 17, 2025, 6:36 p.m.*

Comments

ghingo Highly Voted 8 months, 4 weeks ago
Selected Answer: A
https://learn.microsoft.com/en-us/purview/ome-advanced-expiration
upvoted 10 times

f5831d6 Highly Voted 9 months ago
Selected Answer: A
It's a custom OME Template https://learn.microsoft.com/en-us/purview/ome-advanced-expiration
upvoted 6 times

ageeeeeee Most Recent 1 month, 1 week ago
Selected Answer: C
Steps to start with
Enable Azure Rights Management: Go to Microsoft Purview compliance portal → Information Protection → Activate Rights Management.
Create or edit a sensitivity label: Configure the label to apply encryption and set content expiration (e.g., 7 days).
Publish the label to users: Ensure the label is available in Outlook so senders can apply it when composing emails.
upvoted 1 times

337257e 2 months, 3 weeks ago

Selected Answer: A

Why B. a mail flow rule is not first:
A mail flow rule (also called a transport rule) is used to apply encryption or branding after the configuration exists. It's like assigning a job to a tool—but if the tool hasn't been built yet, the rule has nothing to apply.

In this case:

You want encrypted emails to expire in 7 days or be revoked.

That behavior is only possible through Advanced Message Encryption (AME).

AME settings like expiration and revocation are configured in a custom branding template (via New-OMEConfiguration or Set-OMEConfiguration).

So if you create a mail flow rule first, it won't have the necessary branding template to reference. You'd be pointing to a non-existent configuration.

upvoted 2 times

dmoorthy 3 months ago

Selected Answer: A

New-OMEConfiguration -Identity "Expire in 7 days" -ExternalMailExpiryInDays 7

upvoted 2 times

Nurob 3 months, 2 weeks ago

Selected Answer: B

It is a bit tricky as you have multiple ways to achieve the same result but a Mail Flow should be the correct answer for SC-401
https://learn.microsoft.com/en-us/purview/revoke-ome-encrypted-mail

upvoted 1 times

deeptha92 3 months, 2 weeks ago

Selected Answer: A

A custom branding template is the correct answer.
https://learn.microsoft.com/en-us/purview/ome-advanced-expiration#create-a-custom-branding-template-to-force-mail-expiration-by-using-powershell

This lets us set the external e-mail expiry time in Days.

upvoted 1 times

454252dfr 4 months, 1 week ago

Selected Answer: C

Microsoft 365 sensitivity labels (via Microsoft Purview Information Protection) allow you to:

Apply encryption with access restrictions.

Set content expiration (e.g., revoke access after 7 days).

Define who can access the email and for how long (even after it is delivered).

upvoted 1 times

454252dfr 4 months, 2 weeks ago

Selected Answer: B

The mail flow rule is the first and most direct step to automatically enforce the encryption and expiration requirements for emails sent to external recipients. The rule would be configured to apply an Office 365 Message Encryption (OME) template that has the 7-day expiration policy built-in.

upvoted 1 times

DrArjunReddy 4 months, 2 weeks ago

Selected Answer: B

B should be the right answer. The only way to revoke a message is through mailflow rule. Also let you expire a message.

upvoted 1 times

landfils 5 months, 1 week ago

Selected Answer: C

Sensitivity Label. Custom branding is for user experience in AIP and encryption emails (logo, colors)

upvoted 1 times

CuentaRM10 6 months ago

Selected Answer: A

The answer is correct

upvoted 2 times

Skippy1969 8 months, 2 weeks ago

Selected Answer: C

To ensure that encrypted email messages sent to an external recipient can be revoked or will expire within seven days, you should configure:

C. a sensitivity label

Sensitivity labels in Microsoft 365 allow you to classify and protect your organization's data. By configuring a sensitivity label with specific settings for encryption, you can set expiration policies and revocation options for emails sent to external recipients. This is the most appropriate choice for managing the encryption and expiration of emails.

Additional Context:
Custom Branding Template (A): This is used for branding purposes and does not affect email encryption or expiration.
Mail Flow Rule (B): While mail flow rules can control the flow of emails, they do not provide the specific functionality for revocation or expiration of encrypted messages.
Conditional Access Policy (D): This is used to manage access to resources based on conditions but does not directly relate to email encryption or expiration.

upvoted 2 times

EXAMTOPICS

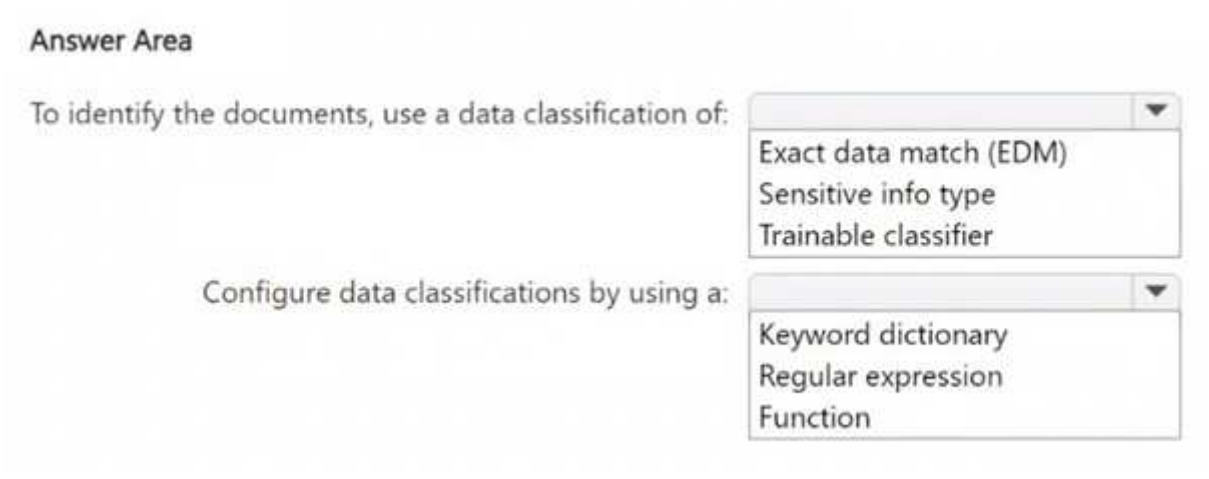
Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 14 DISCUSSION

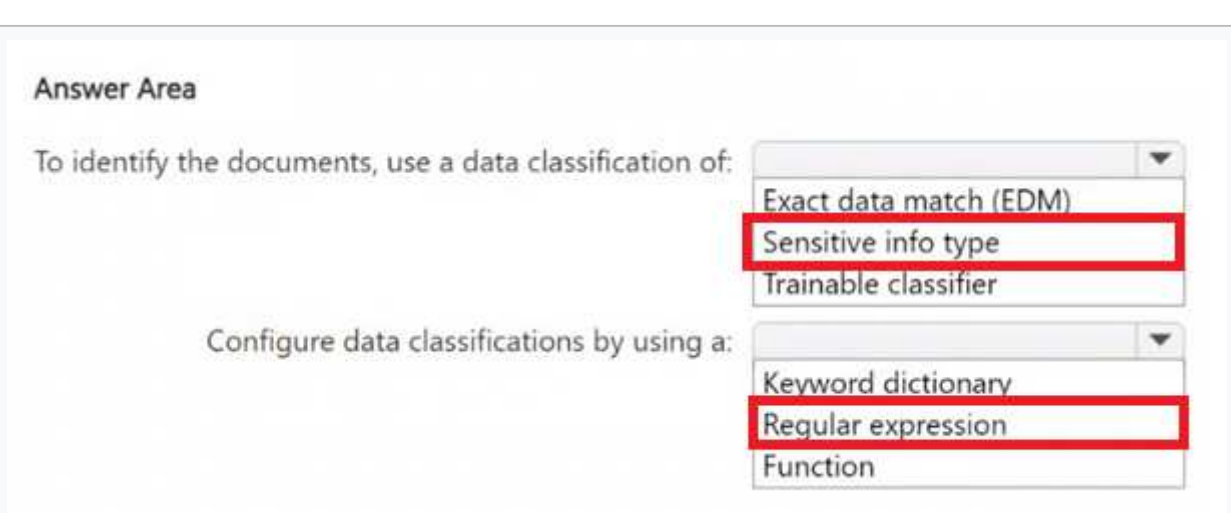
Actual exam question from Microsoft's SC-401
Question #: 14
Topic #: 1
[All SC-401 Questions]

HOTSPOT -
You have a Microsoft 365 E5 subscription.
You need to identify documents that contain patent application numbers containing the letters PA followed by eight digits, for example, PA 12345678. The solution must minimize administrative effort.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Hide Answer

Suggested Answer:



by CuentaRM10 at *May 27, 2025, 1 p.m.*

Comments

CuentaRM10 Highly Voted 6 months, 2 weeks ago
The answer given is correct

upvoted 8 times

dmoorthy Most Recent 3 months ago

Answer is correct. Specific patterns needs Regex. Regex used in SIT.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 16 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 16
Topic #: 1
[All SC-401 Questions]

HOTSPOT -
You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Type
Group1	Microsoft 365
Group2	Security

The subscription contains the resources shown in the following table.

Name	Type
Site1	Microsoft SharePoint Online site
Team1	Microsoft Teams team

You create a sensitivity label named Label1.
You need to publish Label1 and have the label apply automatically.
To what can you publish Label1, and to what can Label1 be auto-applied? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

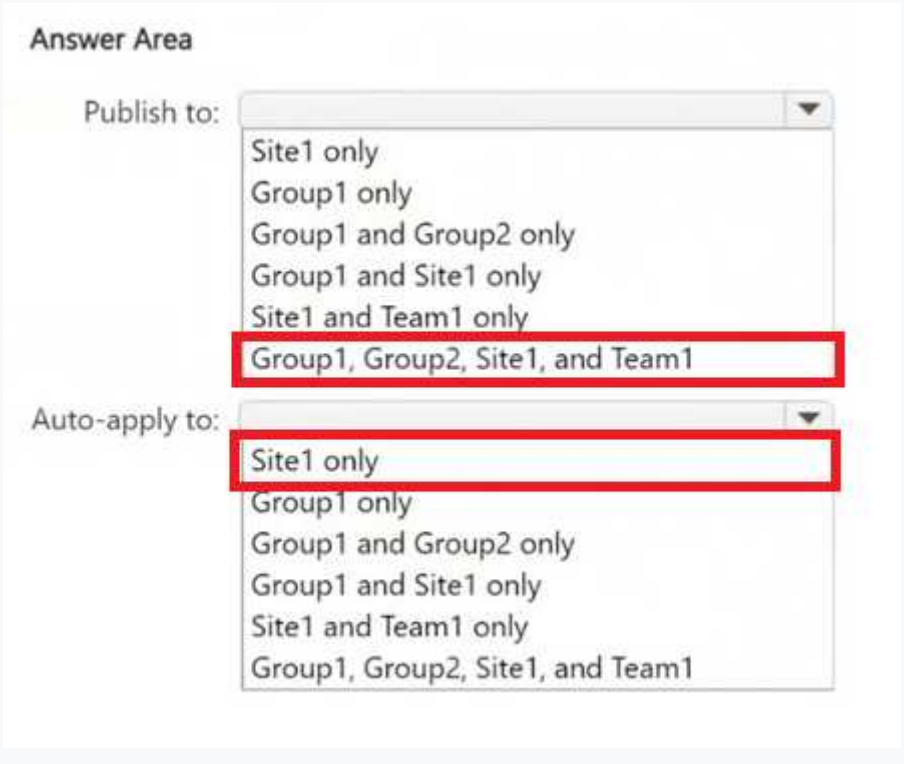
Answer Area

Publish to:
- Site1 only
- Group1 only
- Group1 and Group2 only
- Group1 and Site1 only
- Site1 and Team1 only
- Group1, Group2, Site1, and Team1

Auto-apply to:
- Site1 only
- Group1 only
- Group1 and Group2 only
- Group1 and Site1 only
- Site1 and Team1 only
- Group1, Group2, Site1, and Team1

Hide Answer

Suggested Answer:



by Jarem at *May 31, 2025, 5:30 p.m.*

Comments

gabbinu Highly Voted 3 months, 3 weeks ago

Publish to: Group1 only
Auto-apply to: Site1 only

https://learn.microsoft.com/en-us/purview/sensitivity-labels
Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group (which can have dynamic membership) in Microsoft Entra ID.

Supported locations for auto-labeling include:
• SharePoint Online sites
• OneDrive accounts
• Exchange Online mailboxes
Team1 is a Microsoft Teams team, and while it uses SharePoint for file storage, auto-labeling is not applied to the Team itself, only to the documents stored in its associated SharePoint site.

upvoted 6 times

DrArjunReddy Most Recent 4 months, 2 weeks ago

Group 1
Site 1 and Team 1

U can't publish a label to a security group unless it's mail enabled. You can auto classify files in a site or team enabled site. Also can classify containers.

upvoted 2 times

zied01 4 months, 3 weeks ago

we can't publish label to classic security groups without mail enabled

upvoted 2 times

landfils 5 months, 1 week ago

publish to group1 only
auto-apply to site1 and team1 only

upvoted 3 times

apasxalidou 6 months, 1 week ago

publish to group1 and group2 only
auto-apply to site1 and team1 only

upvoted 2 times

KrisDeb 6 months ago

You can't publish to 'just' the security group but only to mail-enabled security group and it's unclear which one is it as always with those questions.

upvoted 3 times

Jarem 6 months, 2 weeks ago

Copilot Say:
Publish To: Group1 y Group2.
Auto-aply: Site1 y Team1.

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 17 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 17
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

You have a Microsoft 365 ES subscription that uses Microsoft Exchange Online and Teams.

You need to ensure that when a user sends a message containing a cloud attachment, a retention label is applied to the cloud attachment by using an auto-labeling policy.

How should you configure the retention label to start the retention period, and to which locations should you apply the auto-labeling policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Start the retention period based on when the items were:
- Created
- Labeled
- Last modified

Locations:
- Microsoft 365 Group mailboxes & sites only
- OneDrive accounts and SharePoint classic and communication sites only
- Microsoft 365 Group mailboxes & sites, OneDrive accounts, and SharePoint classic and communication sites only

Hide Answer

Suggested Answer:

Answer Area

Start the retention period based on when the items were: Labeled

Locations: Microsoft 365 Group mailboxes & sites only

by tonynoatectron at *Aug. 22, 2025, 2:12 p.m.*

Comments

gabbinu Highly Voted 3 months, 2 weeks ago

Start the retention period: Labeled
Locations: Microsoft 365 Group mailboxes & sites, OneDrive accounts, and SharePoint classic and communication sites only

The auto-labeling policy must be able to label the cloud attachment itself (stored in SharePoint/OneDrive). Starting the period when labeled makes it begin at the moment the auto-label is applied as the message is sent.

upvoted 9 times

tonynoatectron Highly Voted 3 months, 3 weeks ago

Start the retention period based on when the items were: Created

Locations: Microsoft 365 Group mailboxes & sites, OneDrive accounts, and SharePoint classic and communication sites only

upvoted 7 times

Eltooth Most Recent 2 months, 3 weeks ago

Labeled
Microsoft 365 Group mailboxes & sites, OneDrive accounts, and SharePoint classic and communication sites only

upvoted 3 times

Gtc_ 3 months, 1 week ago

Labeled & All locations.

Policies start when items were created, but labels only start when the items were labeled.

https://learn.microsoft.com/en-us/purview/retention?tabs=table-overriden

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 18 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 18
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

You create a data loss prevention (DLP) policy that meets the following requirements:

• Prevents guest users from accessing a sensitive document shared during a Microsoft Teams chat
• Prevents guest users from accessing a sensitive document stored in a Microsoft Teams channel

Which location should you select for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Prevents quest users from accessing a sensitive document shared during a Microsoft Teams chat:

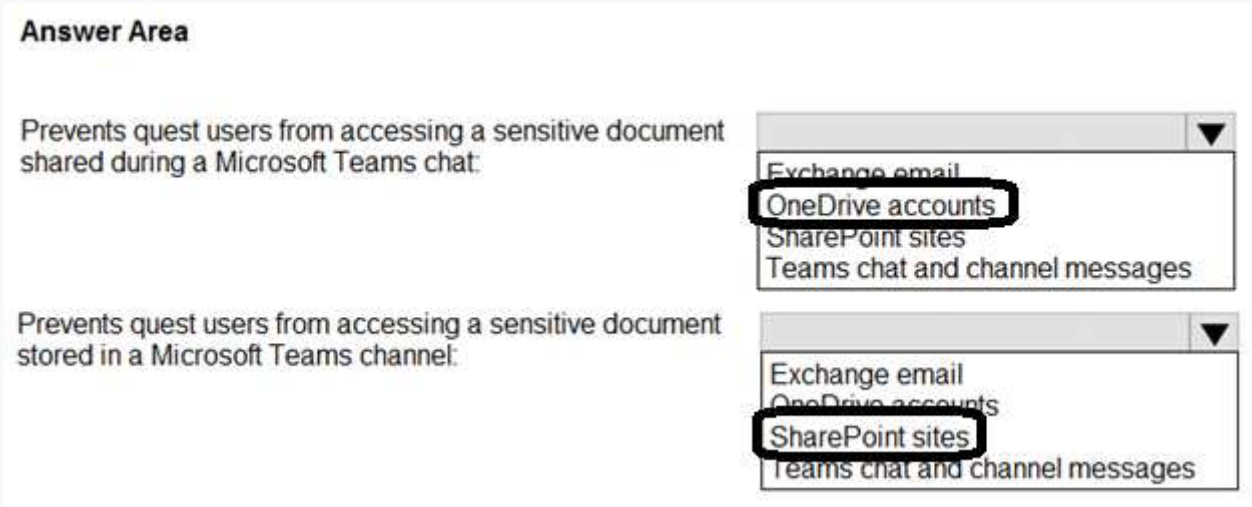
- Exchange email
- OneDrive accounts
- SharePoint sites
- Teams chat and channel messages

Prevents quest users from accessing a sensitive document stored in a Microsoft Teams channel:

- Exchange email
- OneDrive accounts
- SharePoint sites
- Teams chat and channel messages

Hide Answer

Suggested Answer:


Answer Area
Prevents quest users from accessing a sensitive document shared during a Microsoft Teams chat:
OneDrive accounts
SharePoint sites
Teams chat and channel messages
Prevents quest users from accessing a sensitive document stored in a Microsoft Teams channel:
Exchange email
SharePoint sites
Teams chat and channel messages

by Kamiles at *Aug. 25, 2025, 3:32 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

ONeDrive
Sharepoint
https://learn.microsoft.com/en-us/purview/dlp-microsoft-teams
Protecting sensitive information in documents. Suppose that someone attempts to share a document with guests in a Microsoft Teams channel or chat, and the document contains sensitive information. If you have a DLP policy defined to prevent this, the document won't open for those users. Your DLP policy must include SharePoint and OneDrive in order for protection to be enforced. This is an example of DLP for SharePoint that shows up in Microsoft Teams, and therefore requires that users are licensed for Office 365 DLP (included in Office 365 E3), but doesn't require that users be licensed for Office 365 Advanced Compliance.

upvoted 3 times

gabbinu 3 months, 2 weeks ago

Given answers are correct

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 19 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 19
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

You have a Microsoft 365 E5 subscription that uses Microsoft Purview.

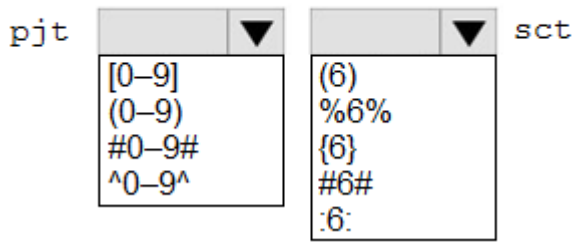
You need to create a sensitive information type (SIT) to detect project code content that starts with the letters pjt followed by six digits and ends with the letters sct. The following is an example of the project code.

pjt123456sct

How should you complete the regular expression? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

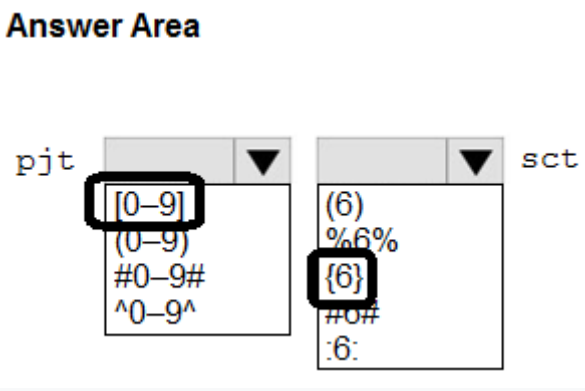
Answer Area



Hide Answer

Suggested Answer:

Answer Area



by Kamiles at *Aug. 25, 2025, 3:34 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

Answer is correct: pjt[0-9]{6}sct

The regular expression pjt[0-9]{6}sct is the correct syntax for detecting a project code that starts with "pjt", contains exactly six digits, and ends with "sct".
Here is a breakdown of the components:
pjt: Matches the literal characters "pjt".
[0-9]: This is a character class that matches any single digit from 0 through 9.
{6}: This is a quantifier that specifies the preceding element ([0-9]) must occur exactly 6 times.
sct: Matches the literal characters "sct".

upvoted 3 times

deeptha92 3 months, 2 weeks ago

pjt[0-9]{6}sct

Given answer is correct

upvoted 2 times

gabbinu 3 months, 2 weeks ago

Given answer is correct

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 20 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 20
Topic #: 1
[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that contains a Windows 11 device named Device1 and three users named User1, User2, and User3.

You plan to deploy Azure information Protection (AIP) and the Microsoft Purview information Protection client to Device1.

You need to ensure that the users can perform the following actions on Device1 as part of the planned deployment:

- User1 will test the functionality of the client.
- User2 will install and configure the Microsoft Rights Management connector.
- User3 will be configured as the service account for the information protection scanner.

The solution must maximize the security of the sign-in process for the users.

What should you do?

A. Exclude User1 and User2 from multifactor authentication (MFA).

B. Enable User2 and User3 for passwordless authentication.

C. Exclude User2 and User3 from multifactor authentication (MFA). Most Voted

D. Enable User1, User2, and User3 for passkey (FIDO2) authentication.

Hide Answer

Suggested Answer: *C*

Community vote distribution

C (67%) D (33%)

by 454252dfr at *Aug. 21, 2025, 5:48 p.m.*

Comments

Eltooth 2 months, 3 weeks ago

Selected Answer: C

User1 can have MFA.
User 3 (service account) can only run with a complex password and NO MFA.
https://learn.microsoft.com/en-us/purview/rights-management-requirements#rights-management-connector-and-mfa

"The Rights Management connector and the Microsoft Purview Information Protection scanner don't support MFA."
upvoted 2 times

skalolaz 3 months, 1 week ago

Selected Answer: C

Rights Management connector and MFA
The Rights Management connector and the Microsoft Purview Information Protection scanner don't support MFA.

If you deploy the connector or scanner, the following accounts mustn't require MFA:

The account that installs and configures the connector.
The service principal account in Microsoft Entra ID, Aadrm_S-1-7-0, that the connector creates.
The service account that runs the scanner.
https://learn.microsoft.com/en-us/purview/rights-management-requirements#rights-management-connector-and-mfa
upvoted 2 times

RickySmith 3 months, 1 week ago

Selected Answer: C

https://learn.microsoft.com/en-us/azure/information-protection/requirements-azure-ad#rights-management-connector-requirements
upvoted 3 times

gabbinu 3 months, 2 weeks ago

Selected Answer: C

Only User1 (tests client) keeps MFA, the RMS connector and the Purview Information Protection scanner do not support MFA and the accounts involved must not require MFA.
https://learn.microsoft.com/en-us/azure/information-protection/requirements-azure-ad
upvoted 3 times

choukou 3 months, 3 weeks ago

Selected Answer: D

la bonne réponse
upvoted 1 times

tonynoatectron 3 months, 3 weeks ago

Selected Answer: D

authentication (FIDO2 (passkey) is the most secure and modern passwordless authentication option.
It maximizes security, applies to all involved users, and is consistent with the need to strengthen the sign-in process.
upvoted 4 times

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 21 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 21

Topic #: 1

[All SC-401 Questions]

HOTSPOT

-

You use project codes that have a format of three alphabetical characters that represent the project type, followed by three digits, for example Abc123.

You need to create a new sensitive info type for the project codes.

How should you configure the regular expression to detect the content? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

(\s)([aA]{3} / [abc]{3} / [alpha]{3} / [a–zA-Z]{3}) \ (d{000-999} / d{123} / d{3})(\s)

Hide Answer

Suggested Answer:

Answer Area

(\s)([aA]{3} / [abc]{3} / [alpha]{3} / [a–zA-Z]{3}) \ (d{000-999} / d{123} / d{3})(\s)

by Kamiles at *Aug. 25, 2025, 3:36 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

You should configure the regular expression as [a-zA-Z]{3}\d{3}

upvoted 3 times

gabbinu 3 months, 2 weeks ago

Given answer is correct

upvoted 2 times

EXAMTOPICS

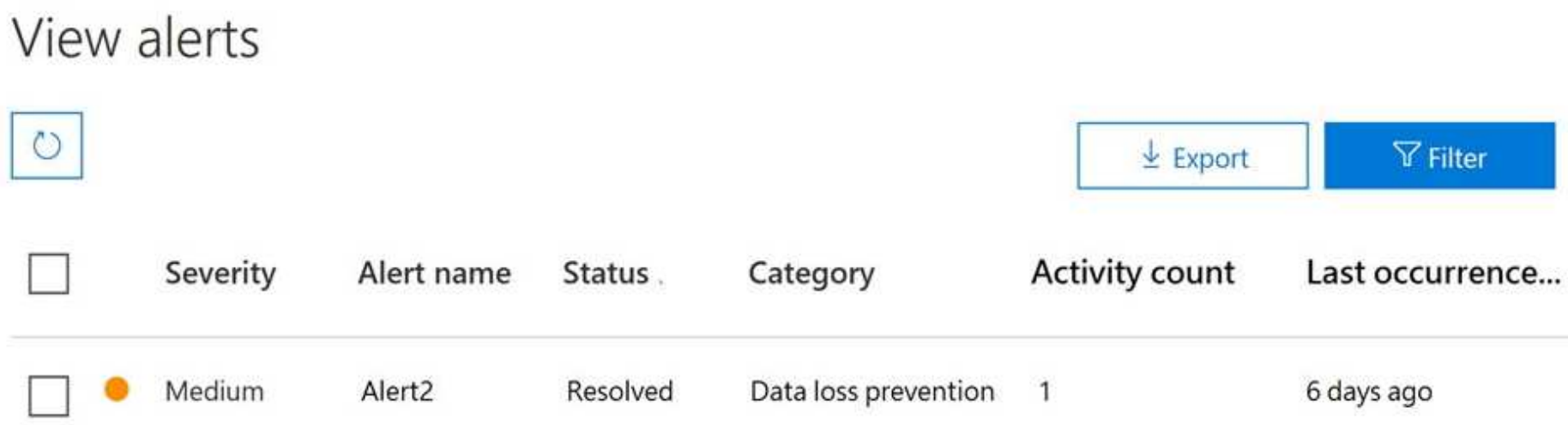
Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 22 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 22
Topic #: 1
[All SC-401 Questions]

You have a Microsoft 365 alert named Alert2 as shown in the following exhibit.



You need to manage the status of Alert2.

To which status can you change Alert2?

A. The status cannot be changed.

B. Dismissed only

C. Investigating only

D. Active or Investigating only

E. Investigating, Active, or Dismissed Most Voted

Hide Answer

Suggested Answer: *E*

Community vote distribution

E (71%) A (29%)

by 454252dfr at *Aug. 21, 2025, 5:53 p.m.*

Comments

f2b34cb 1 month, 1 week ago

Selected Answer: E

You can change a resolved alert in 365 DLP to the Dismissed or Active status. While the standard workflow moves an alert to a "resolved" state when it's handled, you can also dismiss it if it's not relevant or reopen it to an active status if further action is needed.
Dismissed: Use this status if the alert is not relevant, was a false positive, or has already been dealt with in a way that doesn't require further investigation.
Active: Revert an alert to this status if a review reveals that it was incorrectly resolved and requires more action.
Investigating: This is a status to use when you are actively working on the alert.

upvoted 2 times

Alcpt 1 month, 2 weeks ago

Selected Answer: A

A resolved alert will not change its status, but the associated alert policy can still create new alerts if the triggering conditions are met again.

upvoted 1 times

Alcpt 3 weeks, 2 days ago

Updating my answer to E
Yes, you can change a Resolved alert's status back to Active, Investigating (or In Progress), or Dismissed within the Microsoft 365 portals. While "Resolved" signifies that an investigation is complete, you might need to change the status if new information emerges or if the issue recurs

upvoted 1 times

Eltooth 2 months, 3 weeks ago

Selected Answer: A

There is no clear answer to this as the official MS documentation has changed.
"The official Microsoft documentation on the lifecycle of DLP alerts does not explicitly state that a resolved alert can never be reopened or changed to another status. However, it does describe the process as moving through stages like Trigger → Notify → Triage → Investigate → Remediate → Tune, and once remediation is complete, the alert is considered closed. The documentation emphasizes that the Microsoft Defender portal retains incidents for six months, and the DLP alert management dashboard retains alerts for 30 days, but it does not mention an option to revert a resolved alert back to an active state.1

So, while the statement you provided is mostly accurate in practice (resolved alerts are treated as final), Microsoft does not explicitly say “cannot be reopened” in the docs. It’s more about the workflow being designed for forward progression rather than reopening."

upvoted 1 times

454252dfr 3 months, 3 weeks ago

Selected Answer: E

Correct

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 23 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 23
Topic #: 1
[All SC-401 Questions]

You have a Microsoft 365 subscription that uses retention label policies.

You need to identify all the changes made to retention labels during the last 30 days.

What should you use in the Microsoft Purview portal?

A. Reports
B. Activity explorer Most Voted
C. Content search
D. Use data search

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (100%)

by 454252dfr at *Aug. 21, 2025, 5:55 p.m.*

Comments

454252dfr Highly Voted 3 months, 3 weeks ago

Selected Answer: B

Correct

upvoted 7 times

Eltooth Most Recent 2 months, 3 weeks ago

Selected Answer: B

B is correct answer.

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 24 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 24

Topic #: 1

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that contains a user named User1.

You deploy Microsoft Purview Data Security Posture Management for AI (DSPM for AI).

You need to ensure that User1 can verify the auditing status of the subscription. The solution must follow the principle of least privilege.

To which role group should you add User1?

A. Security Reader Most Voted

B. Insider Risk Management Analysts

C. Insider Risk Management Investigators

D. View-Only Organization Management for Microsoft Exchange Online

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (58%) D (42%)

by 454252dfr at *Aug. 21, 2025, 5:56 p.m.*

Comments

gabbinu Highly Voted 3 months, 2 weeks ago

Selected Answer: D

https://learn.microsoft.com/en-us/purview/audit-log-enable-disable
To verify tenant auditing you just need to read the setting UnifiedAuditLogIngestionEnabled (e.g., with Get-AdminAuditLogConfig). The View-Only Organization Management role group includes the View-Only Configuration role, which is sufficient to read that auditing status.

upvoted 8 times

454252dfr Highly Voted 3 months, 3 weeks ago

Selected Answer: A

The correct role group to add User1 to is A. Security Reader.

The Security Reader role group provides read-only access to security-related reports and data in Microsoft 365, including auditing logs. This role aligns with the principle of least privilege, as it allows User1 to verify the auditing status without granting them permissions to modify settings or

access sensitive content beyond what is necessary for their task. The other options grant broader permissions or are specific to different areas of compliance that don't directly relate to verifying the general auditing status of the subscription.

upvoted 8 times

Jideakin Most Recent 2 weeks, 6 days ago

Selected Answer: A

Correct Answer is A.

The specific role (or permission) required to view auditing status is the "View-Only Manage Alerts" and Security Reader is the only Role Group of all the listed that includes it.
https://learn.microsoft.com/en-us/defender-office-365/scc-permissions

View-Only Organization Management: Members can view the properties of any object in the Exchange Online organization; not tenant setting like audit status.
https://learn.microsoft.com/en-us/exchange/permissions-exo/permissions-exo

upvoted 2 times

Eltooth 2 months, 3 weeks ago

Selected Answer: A

A is correct answer : Security Reader

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 25 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 25
Topic #: 1
[All SC-401 Questions]

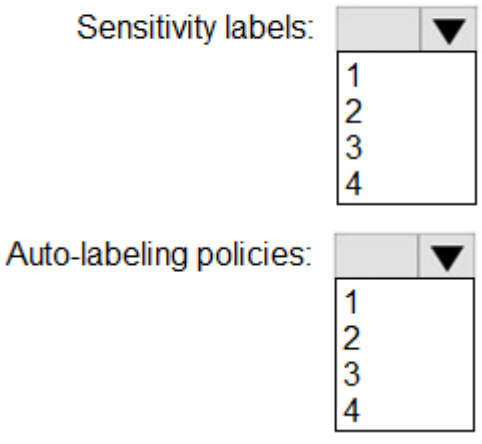
HOTSPOT
-

You need to implement an information compliance policy to meet the following requirements:

• Documents that contain passport numbers from the United States, Germany, Australia, and Japan must be identified automatically.
• When a user attempts to send an email or an attachment that contains a passport number, the user must receive a tooltip in Microsoft Outlook.
• Users must be blocked from using Microsoft SharePoint Online or OneDrive for Business to share a document that contains a passport number.

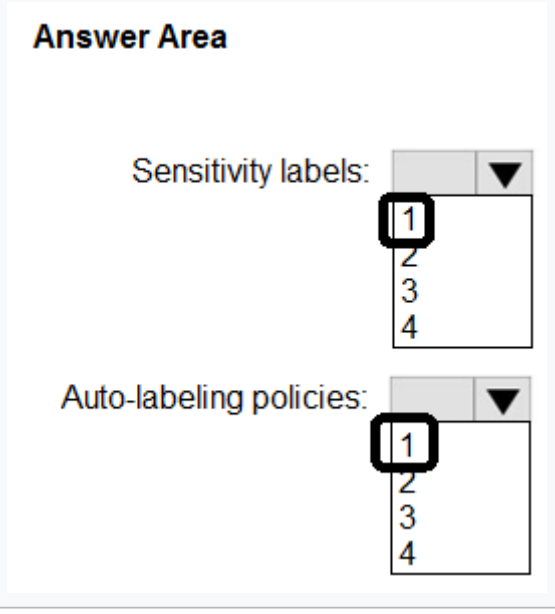
What is the minimum number of sensitivity labels and auto-labeling policies you should create? To answer, select the appropriate options in the answer area.

Answer Area



Hide Answer

Suggested Answer:



by Kamiles at *Aug. 25, 2025, 3:36 a.m.*

Comments

deeptha92 Highly Voted 3 months, 2 weeks ago

1, 1

One sensitivity label to capture the United States, Germany, Australia, and Japan passport numbers (Microsoft defined SITs can be used to create the label). Then this label can be used to automatically identify and label documents with the said passport numbers. Tooltip when sending an attachment that contains a passport number can be done with a DLP policy, as well as blocking users from sharing files containing a passport number.

upvoted 7 times

Eltooth Most Recent 2 months, 3 weeks ago

1 Sensitivity label & 1 Auto-labeling policy
Use built-in sensitive information types (SITs) for the passport numbers of the United States, Germany, Australia, and Japan. A single sensitivity label can be configured to use multiple SITs.
Define the permissions and restrictions. To meet the requirements, the label should be configured to prevent external sharing for files in SharePoint and OneDrive.
Auto-labeling policy
Target the locations Exchange Online (for emails), SharePoint Online, and OneDrive for Business.
Apply the "Passport Numbers - Confidential" sensitivity label when content matches any of the conditions, which will be the sensitive information types for the four countries' passport numbers.
Configure a user notification with a custom message to appear as a tooltip in Outlook when the label is auto-applied to an email or attachment.
Block external sharing for files in SharePoint Online and OneDrive for Business by enforcing the label's configured restrictions.

upvoted 3 times

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 26 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 26
Topic #: 1
[All SC-401 Questions]

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You recently discovered that the developers at your company emailed Azure Storage Account keys in plain text to third parties.

You need to ensure that when Azure Storage Account keys are emailed, the emails are encrypted.

Solution: You create a data loss prevention (DLP) policy that has Exchange email, SharePoint sites, OneDrive accounts, and Teams chat and channel messages selected.

Does this meet the goal?

A. Yes

B. No Most Voted

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (83%) A (17%)

by Kamiles at *Aug. 25, 2025, 3:33 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

Selected Answer: B

B is correct answer: OME or a mail flow rule is required.

upvoted 1 times

skalolaz 3 months ago

Selected Answer: A

DLP can block or encrypt data in M365.

upvoted 1 times

evrybobry 1 month, 1 week ago

When Exchange email, SharePoint sites, OneDrive accounts, and Teams chat and channel messages is selected you don't have an action to encrypt.

upvoted 3 times

Nurob 3 months, 2 weeks ago

Selected Answer: B

DLP Policy alone does not enforce e-mail encryption, you need OME or Mail flow Rule

upvoted 1 times

Suranka 3 months, 2 weeks ago

Selected Answer: B

DLP policy alone does not automatically encrypt emails. For encryption, you need Microsoft Purview Message Encryption (OME) configured through a sensitivity label or a mail flow rule (transport rule) in Exchange.

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 27 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 27
Topic #: 1
[All SC-401 Questions]

DRAG DROP
-

You have a Microsoft 365 E5 subscription.

You need to label Microsoft Exchange Online emails that match the following conditions:

- Contain employment offers
- Contain offensive language
- Contain medical terms and conditions

The solution must minimize administrative effort.

Which type of data classification should you use for each condition? To answer, drag the appropriate data classification types to the correct conditions. Each data classification type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Data classifications	Answer Area	
Exact data match (EDM)	Contain employment offers:	
Sensitive info type	Contain offensive language:	
Trainable classifier	Contain medical terms and conditions:	

Hide Answer

Suggested Answer:

Answer Area	
Contain employment offers:	Sensitive info type
Contain offensive language:	Trainable classifier
Contain medical terms and conditions:	Exact data match (EDM)

by Kamiles at *Aug. 25, 2025, 3:36 a.m.*

Comments

gabbinu Highly Voted 3 months, 2 weeks ago

Contain employment offers → Trainable classifier
(Unstructured content; best caught by a classifier trained on examples.)

Contain offensive language → Trainable classifier
(Semantic/phrase-based detection fits a classifier, not SIT/EDM.)

Contain medical terms and conditions → Sensitive info type
(Use a SIT with keyword dictionary/phrases for the medical T&Cs.)

upvoted 7 times

RickySmith Most Recent 2 months, 2 weeks ago

3 - https://learn.microsoft.com/en-us/purview/trainable-classifiers-definitions
3 - https://learn.microsoft.com/en-us/purview/trainable-classifiers-definitions
2 - https://learn.microsoft.com/en-us/purview/sit-defn-all-medical-terms-conditions

upvoted 3 times

Eltooth 2 months, 3 weeks ago

Trainable
Trainable
SIT

upvoted 1 times

choukou 3 months, 2 weeks ago

Solution : 1: Trainable
2 : Trainable
3: SIT

upvoted 3 times

Gtc_ 3 months, 2 weeks ago

I would think trainable, trainable, SIT.

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam

Go to Exam

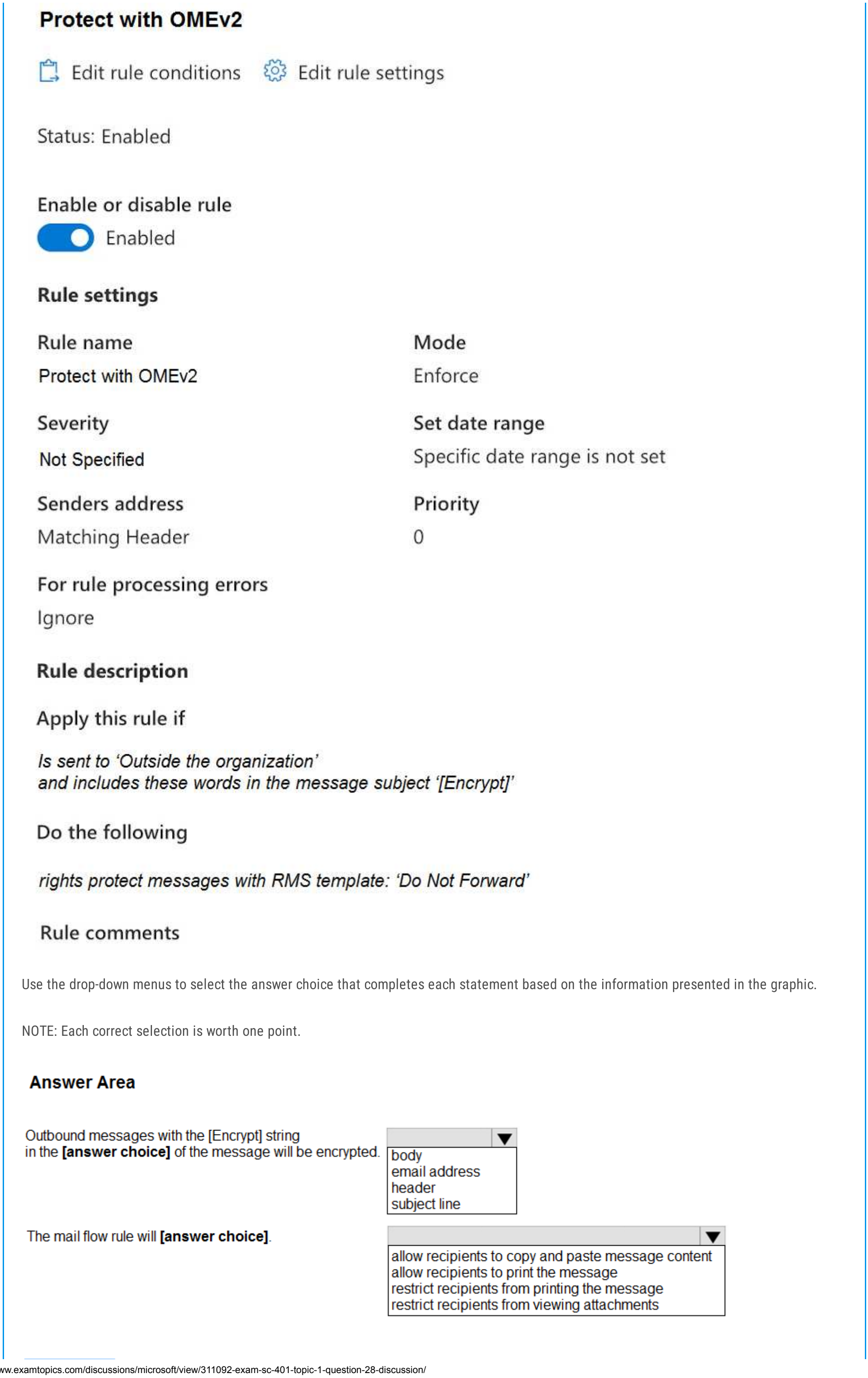
EXAM SC-401 TOPIC 1 QUESTION 28 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 28
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

You have a Microsoft 365 E5 subscription.

In Microsoft Exchange Online, you have the mail flow rule shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

Outbound messages with the [Encrypt] string in the **[answer choice]** of the message will be encrypted.

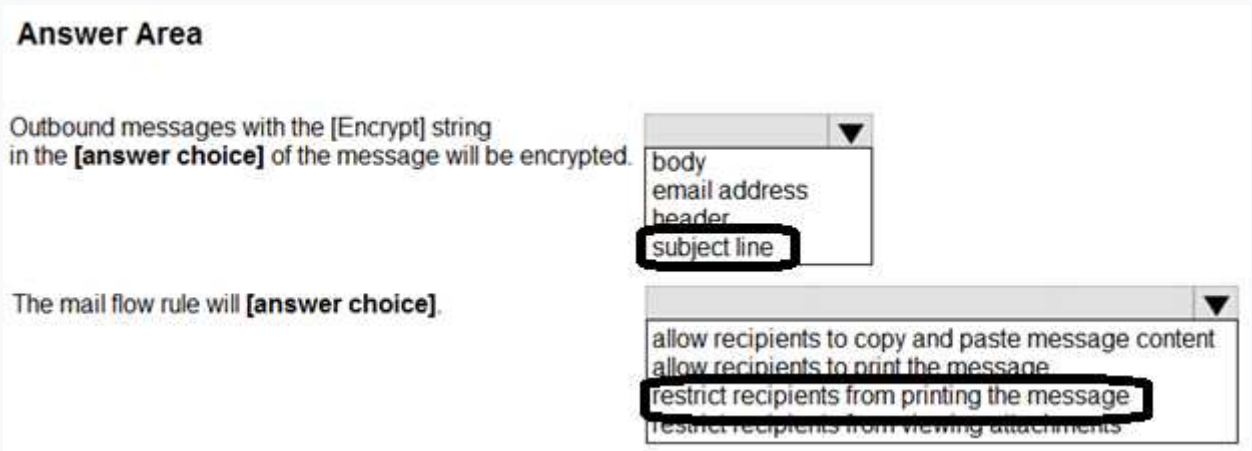
- body
- email address
- header
- subject line

The mail flow rule will **[answer choice]**.

- allow recipients to copy and paste message content
- allow recipients to print the message
- restrict recipients from printing the message
- restrict recipients from viewing attachments

Hide Answer

Suggested Answer:


Answer Area
Outbound messages with the [Encrypt] string in the [answer choice] of the message will be encrypted.
body
email address
header
subject line
The mail flow rule will [answer choice].
allow recipients to copy and paste message content
allow recipients to print the message
restrict recipients from printing the message

by Kamiles at *Aug. 25, 2025, 3:35 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Answer is correct.
Subject line
Prevent users from printing

upvoted 4 times

gabbinu 3 months, 2 weeks ago

Given answers are correct.
The rule triggers on messages sent outside the org that have [Encrypt] in the subject. The action applies the Do Not Forward RMS template, which blocks forwarding, copying, and printing.

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 29 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 29
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

You have a Microsoft 365 5 subscription that contains the devices shown in the following table.

Name	Platform	Chipset
Device1	Windows 11	x64
Device2	Windows 11	ARM64
Device3	Windows 10	x86

You publish Microsoft Purview Information Protection sensitivity labels.

You plan to deploy the information protection client to the devices. The solution must ensure that the labels can be applied to sensitive images and documents.

On which devices can you install the information protection client, and what should users use to apply labels? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

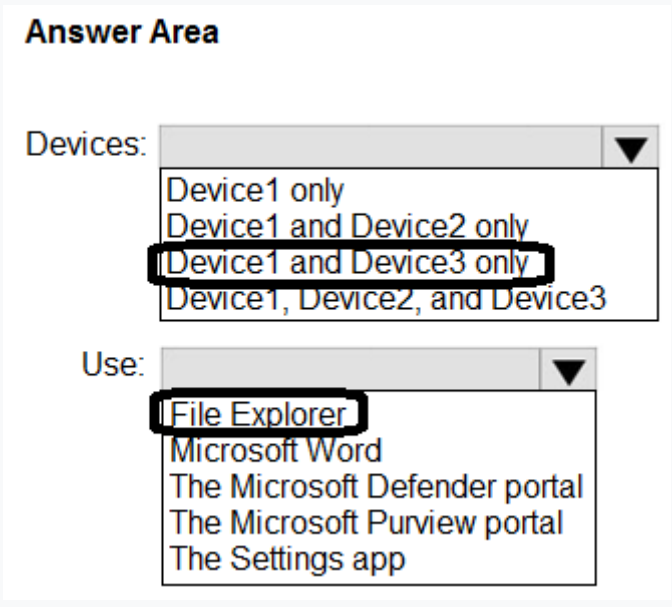
Answer Area

Devices:
- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2, and Device3

Use:
- File Explorer
- Microsoft Word
- The Microsoft Defender portal
- The Microsoft Purview portal
- The Settings app

Hide Answer

Suggested Answer:



by Kamiles at *Aug. 25, 2025, 3:34 a.m.*

Comments

novaCapta 1 week, 4 days ago

ARM64 is supported for the viewer and file labeler. https://learn.microsoft.com/en-us/purview/information-protection-client?tabs=devices%2Cinstall-client-exe%2Cclassification-file-types%2Cexcluded-folders#requirements-for-deploying-the-information-protection-client

upvoted 1 times

Eltooth 2 months, 3 weeks ago

Device 1 & 3
File Explorer

upvoted 2 times

Blabla532 4 days, 18 hours ago

x86 is not supported by Purview client. Device 1 and 2

upvoted 1 times

gabbinu 3 months, 2 weeks ago

Given answers are correct.
The Purview Information Protection (AIP/MIP) client installs only on Windows x86/x64 (not ARM64), so it supports Win11 x64 and Win10 x86, but not Win11 ARM64. To label images and non-Office files, users apply the label via the client's File Explorer right-click ("Classify and protect").

upvoted 3 times

Gtc_ 3 months, 2 weeks ago

Device 1 and file explorer

upvoted 2 times

Gtc_ 3 months, 1 week ago

Device 1 & 3, my mistake in typing this.

upvoted 1 times

Gtc_ 3 months, 2 weeks ago

https://learn.microsoft.com/en-us/purview/information-protection-client?tabs=devices%2Cinstall-client-exe%2Cclassification-file-types%2Cexcluded-folders#requirements-for-deploying-the-information-protection-client

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 30 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 30
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

You have a Microsoft 365 E5 subscription that contains the sensitive information types (SITs) shown in the following table.

Name	Detection method
SIT1	Fingerprint
SIT2	Regular expression

You plan to create the policies shown in the following table and assign them to a Microsoft SharePoint Online site.

Name	Type
DLP1	Data loss prevention (DLP) policy
Retention1	Retention label auto-labeling policy
Sensitivity1	Sensitivity label auto-labeling policy

Which policies can use SIT1, and which policies can use SIT2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

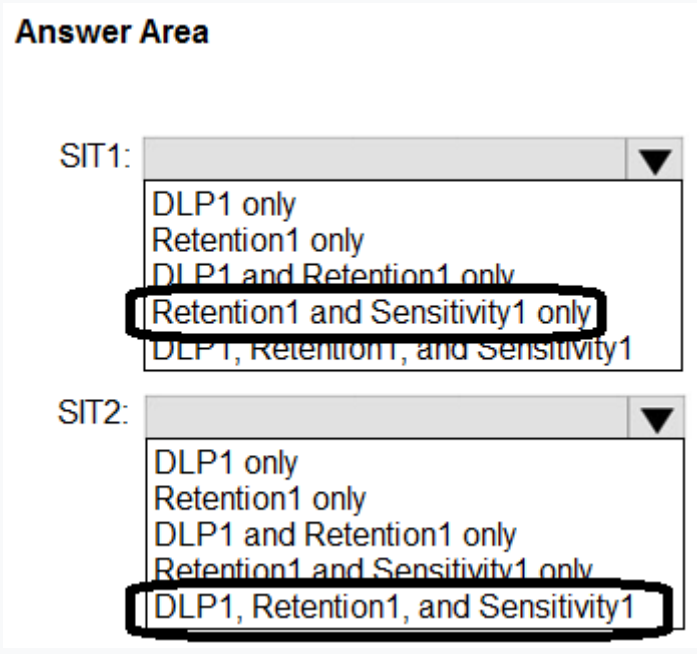
Answer Area

SIT1:
- DLP1 only
- Retention1 only
- DLP1 and Retention1 only
- Retention1 and Sensitivity1 only
- DLP1, Retention1, and Sensitivity1

SIT2:
- DLP1 only
- Retention1 only
- DLP1 and Retention1 only
- Retention1 and Sensitivity1 only
- DLP1, Retention1, and Sensitivity1

Hide Answer

Suggested Answer:



by Kamiles at *Aug. 25, 2025, 3:33 a.m.*

Comments

Jideakin 2 weeks, 3 days ago

Perhaps this is new, as Purview keeps getting updated, but I tested it and Auto-apply Retention Label policy can use Fingerprint-based SIT.
So the correct answer is:
SIT1 = All
SIT2 = All

upvoted 2 times

Ender3 2 months, 1 week ago

gabbinu is right. The options provided for SIT1 are incomplete. There should be an option for DLP and sensitivity auto-labeling.

upvoted 2 times

Eltooth 2 months, 3 weeks ago

SIT1: DLP & Sensitivity
SIT2 DLP, Retention & Sensitivity

upvoted 1 times

gabbinu 3 months, 2 weeks ago

SIT1 (Fingerprint) → DLP and Sensitivity auto-labeling (I don't understand why it's not among the options, since MIP auto-labeling can use document fingerprinting as a detection method in Exchange, SharePoint, and OneDrive.
https://learn.microsoft.com/en-us/purview/sit-document-fingerprinting)

SIT2 (Regex) → DLP, Retention auto-labeling, and Sensitivity auto-labeling.

upvoted 3 times

Nurob 3 months, 2 weeks ago

Fingerprints can only be used with DLP policies, while regex SITs work with DLP, retention, and sensitivity auto-labeling.

upvoted 2 times

Gtc_ 3 months, 2 weeks ago

SIT1: DLP1 only
SIT2: All of them

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 31 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 31
Topic #: 1
[All SC-401 Questions]

You have a Microsoft 365 subscription that contains two Microsoft SharePoint Online sites named Site1 and Site2.

You plan to use policies to meet the following requirements:

- Add a watermark of Confidential to a document if the document contains the words Project1 or Project2.
- Retain a document for seven years if the document contains credit card information.
- Add a watermark of Internal Use Only to all the documents stored on Site2.
- Add a watermark of Confidential to all the documents stored on Site1.

You need to recommend the minimum number of sensitive info types required.

How many sensitive info types should you recommend?

A. 1
B. 2 Most Voted
C. 3
D. 4

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (88%) 12%

by Rtstrider at *Aug. 21, 2025, 5:48 p.m.*

Comments

Suranka Highly Voted 3 months, 2 weeks ago

Selected Answer: B

To meet the requirements described in the image, let's break down the scenarios:

Watermark "Confidential" if document contains "Project1" or "Project2"

This requires 1 custom sensitive info type to detect either "Project1" or "Project2".

Retain document for 7 years if it contains credit card information

This uses 1 built-in sensitive info type (e.g., Credit Card Number).
Watermark "Internal Use Only" for all documents on Site2

This is location-based, not content-based, so no sensitive info type needed.
Watermark "Confidential" for all documents on Site1

Also location-based, so no sensitive info type needed.

upvoted 6 times

Rtstrider Highly Voted 3 months, 3 weeks ago

Selected Answer: B

Project 1 and Project 2 can be added to a single custom Sensitive Info type. The second Sensitive info type would be Credit Card information I would think. For this reason I'm voting B (2) Sensitive Info Types

upvoted 5 times

Ender3 Most Recent 2 months, 1 week ago

Selected Answer: B

Two SITs are needed. Here is why:
1. Create one SIT to identify project 1 and project 2 content. This is used in an auto-labeling policy to apply a sensitivity label for the "Confidential" watermarking.
2. Use a credit card SIT in an auto-labeling policy to apply a 7-year retention label.
3. Apply a sensitivity label to all content stored on Site2 for the "Internal" watermarking. No SIT needed.
4. Apply a sensitivity label to all content stored on Site1 for the "Confidential" watermarking. No SIT needed.

upvoted 1 times

Nurob 3 months, 2 weeks ago

Selected Answer: B

I only see 2 SITs needed: ONE for documents that contains specific words Project1 or Project2, and ONE for Credit Cards, the reset is location based so I don't see the point of a 3rd SIT

upvoted 3 times

choukou 3 months, 2 weeks ago

Selected Answer: U

1 seul

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 32 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 32
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

You have a Microsoft 365 E5 subscription that contains the sensitive information types (SITs) shown in the following table.

Name	Primary element	Character proximity	Supporting elements	Additional checks
SIT1	Regular expression: `prd:\d{4}`	15	Keyword: product	*None*
SIT2	Regular expression: `(\d{10}\d{12})`	*None*	*None*	Exclude specific values: 111-111-1111
SIT3	Function: `Func_credit_card`	*None*	*None*	*None*

A user sends the email messages shown in the following table.

Name	Content
Email1	The product code you requested for the bicycle is prd:1234.
Email2	The bank account number is 123456789012. Contact your account rep at 111-111-1111.
Email3	Please use my credit card that ends with 0023 and has an expiration date of 01/25.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
SIT1 will identify and match the content in Email1.	○	○
SIT2 will identify and match the content in Email2.	○	○
SIT3 will identify and match the content in Email3.	○	○

Hide Answer

Suggested Answer:

Answer Area

Statements	Yes	No
SIT1 will identify and match the content in Email1.	○	○
SIT2 will identify and match the content in Email2.	○	○
SIT3 will identify and match the content in Email3.	○	○

by Kamiles at *Aug. 25, 2025, 3:32 a.m.*

Comments

deeptha92 Highly Voted 3 months, 2 weeks ago

SIT1 on Email1 → No (keyword too far from regex match)

SIT2 on Email2 → No (pattern requires 22 digits, text has only 12)

SIT3 on Email3 → No (only last 4 digits of card number, fails Func_credit_card)

upvoted 9 times

Lapiduse 3 months ago

My answer:
Y - we have a matching regex + supporting keyword: product in the email
N
N

upvoted 6 times

Gtc_ 3 months, 2 weeks ago

Agree with No on all 3

upvoted 2 times

Alcpt Most Recent 3 weeks, 2 days ago

N > the word "product" is > 15 chars away,
Y > 12 numbers as per /d{12} and 111... is ignored
N > no full credit card number in the email

upvoted 2 times

337257e 2 months, 3 weeks ago

The answer shown is correct1. SIT1 will identify and match the content in Email1
✅ Regex prd:\d{4} matches prd:1234

✅ Keyword product is present within 15 characters

✅ All conditions met 👉 Answer: Yes

2. SIT2 will identify and match the content in Email2
✅ Contains 123456789012 → valid 12-digit match

❌ 111-111-1111 is excluded, but it's not the match 👉 Answer: Yes

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 33 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 33
Topic #: 1
[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

On January 1, you create the sensitivity label shown in the following table.

Setting	Value
Name	Label1
Assign permissions now or let users decide?	Assign permissions now
User access to content expires	After 21 days
Assign permissions to specific users and groups	Co-Author: User1 and User2

On January 2, you publish Label1 to User.

On January 3, User1 creates a Microsoft Word document named Doc1 and applies Label1 to the document.

On January 4, User2 edits Doc1.

On January 15, you increase the content expiry period for Label1 to 28 days.

When will access to Doc1 expire for User2?

A. January 23

B. January 24 Most Voted

C. January 25

D. January 31

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (100%)

by Kamiles at *Aug. 25, 2025, 3:34 a.m.*

Comments

gabbinu Highly Voted 3 months, 2 weeks ago

Selected Answer: B

The expiry period is stamped into the document at the time the label is applied.
• Changing the label later does not retroactively update already protected content.
• To take effect, the document must be re-labeled.
So for Doc1, applied on Jan 3 with a 21-day expiry, the countdown is fixed → expiry = Jan 24.

upvoted 6 times

Eltooth Most Recent 2 months, 3 weeks ago

Selected Answer: B

B is correct answer - retention label applies from doc creation I.e. 3rd Jan. plus 21 days =3 weeks Jan 24th.

upvoted 2 times

deeptha92 3 months, 2 weeks ago

Selected Answer: B

Documents already labelled with a sensitivity label will retain the original expiry settings until they reconnect to the service and synchronise with the updated label configuration 1. This would only happen it a user opens the doc.

upvoted 1 times

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 34 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 34

Topic #: 1

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 E5 tenant that contains a trainable classifier named Classifier1.

You need to increase the accuracy of Classifier1. The solution must use the principle of least privilege.

Which feature should you use and to which role group should you be added? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Feature:
- Activity explorer
- Content explorer
- Compliance Manager
- Microsoft Information Governance

Role group:
- Compliance Data Administrator
- Compliance Manager Contributors
- Compliance Manager Readers

Hide Answer

Suggested Answer:

Answer Area

Feature: Content explorer

Role group: Compliance Data Administrator

by Kamiles at *Aug. 25, 2025, 3:34 a.m.*

Comments

Jideakin 2 weeks, 3 days ago

Not sure there's a correct ans here.
Assuming the user already has the:
Data Classification list & Content Viewer roles (which is required to use Content Explorer in the first place)
I would add the Complaince Administrator Role Group to that. It contains the Roles:
Data Classification Feedback Provider, and
Data Classification Feedback Reviewer
which I believe are needed for training the classifier.
Compliance Data Administrator Role Group does not includes these Roles.

upvoted 1 times

Eltooth 2 months, 3 weeks ago

Content Explorer
Data Admin

upvoted 3 times

Gtc_ 3 months, 2 weeks ago

Agree with given answer

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 35 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 35

Topic #: 1

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains the resources shown in the following table.

Name	Type	Member of
User1	User	*None*
User2	User	Group1
Group1	Group	*None*

The subscription contains a Windows 11 device named Device1 and has the Microsoft Purview Information Protection client installed. Device1 contains the resources shown in the following table.

Name	Type	Path
File1.png	File	C:\Temp
File2.docx	File	D:\Folder1
Folder2	Folder	D:\

You publish a sensitivity label named Label1 to User1 and Group1.

For each of the following statements, select Yes if the statement is true, Otherwise, select No.

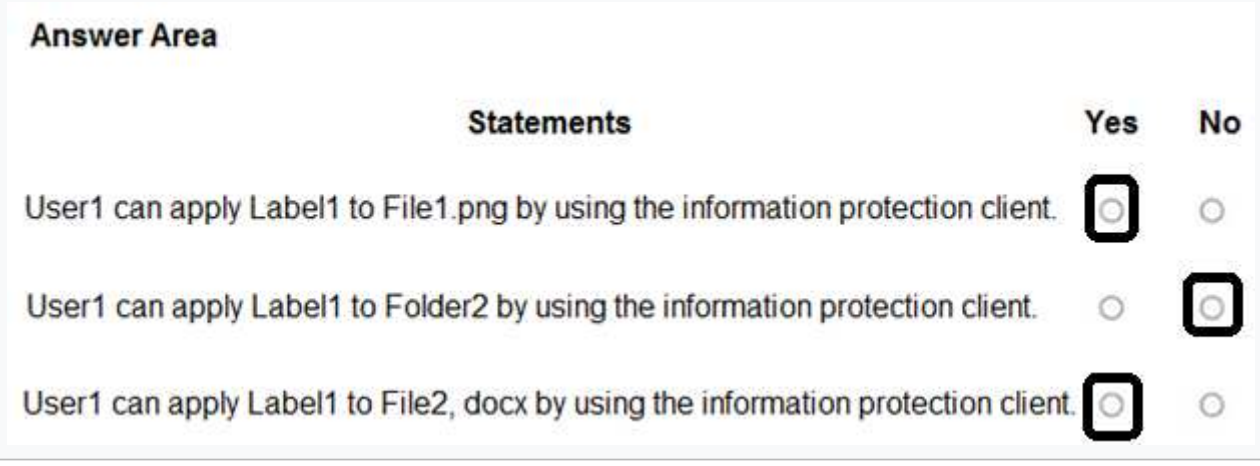
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can apply Label1 to File1.png by using the information protection client.	○	○
User1 can apply Label1 to Folder2 by using the information protection client.	○	○
User1 can apply Label1 to File2, docx by using the information protection client.	○	○

Hide Answer

Suggested Answer:


Answer Area
Statements
Yes
No
User1 can apply Label1 to File1.png by using the information protection client.
User1 can apply Label1 to Folder2 by using the information protection client.
User1 can apply Label1 to File2, docx by using the information protection client.

by Kamiles at *Aug. 25, 2025, 3:35 a.m.*

Comments

gabbinu Highly Voted 3 months, 2 weeks ago

Given answers are correct.
Yes – The Purview Information Protection client (File Explorer "Classify and protect") can label .png and other non-Office files.
No – The client labels files only, not folders.
Yes – The client can label .docx files too (even though Office apps also have the Sensitivity button).

upvoted 6 times

Eltooth Most Recent 2 months, 3 weeks ago

Agreed
Yes
No
Yes

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 36 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 36

Topic #: 1

[All SC-401 Questions]

You have a Microsoft 365 E5 tenant that uses a domain named contoso.com.

A user named User1 sends link-based, branded emails that are encrypted by using Microsoft Purview Advanced Message Encryption to the recipients shown in the following table.

Name	Email address
Recipient1	Recipient1@contoso.com
Recipient2	Recipient2@fabrikam.onmicrosoft.com
Recipient3	Recipient3@outlook.com
Recipient4	Recipient4@gmail.com

For which recipients can User1 revoke the emails?

A. Recipient1 only

B. Recipient4 only Most Voted

C. Recipient1 and Recipient2 only

D. Recipient3 and Recipient4 only

E. Recipient1, Recipient2, Recipient3, and Recipient4

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (80%) D (20%)

by Kamiles at *Aug. 25, 2025, 3:36 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

Selected Answer: B

B is correct answer. Based on explanations below -only gmail would receive link based branded encrypted email that could be revoked.

upvoted 1 times

gabbinu 3 months, 2 weeks ago

Selected Answer: B

https://learn.microsoft.com/en-us/purview/revoke-ome-encrypted-mail
Admins and message senders can revoke encrypted emails if the recipient received a link-based, branded encrypted email. If the recipient received a native inline experience in a supported Outlook client, then you can't revoke the message.

Whether a recipient receives a link-based experience or an inline experience depends on the recipient identity type: Microsoft 365 and Microsoft account recipients (for example, outlook.com users) get an inline experience in supported Outlook clients. All other recipient types, such as Gmail and Yahoo recipients, get a link-based experience.

upvoted 2 times

Gtc_ 3 months, 2 weeks ago

Selected Answer: B

Of the options listed, only Gmail gets link-based.

https://learn.microsoft.com/en-us/purview/revoke-ome-encrypted-mail?utm_source=chatgpt.com

Encrypted emails that you can revoke:
Admins and message senders can revoke encrypted emails if the recipient received a link-based, branded encrypted email. If the recipient received a native inline experience in a supported Outlook client, then you can't revoke the message.

Whether a recipient receives a link-based experience or an inline experience depends on the recipient identity type: Microsoft 365 and Microsoft account recipients (for example, outlook.com users) get an inline experience in supported Outlook clients. All other recipient types, such as Gmail and Yahoo recipients, get a link-based experience.

Admins and message senders can revoke messages that are encrypted using encryption applied directly from Outlook on the web. For example, messages encrypted with the Encrypt Only option."

upvoted 2 times

Suranka 3 months, 2 weeks ago

Selected Answer: D

Based on Microsoft Purview Advanced Message Encryption capabilities, User1 can revoke the emails sent to Recipient3 and Recipient4.

upvoted 2 times

deeptha92 3 months, 2 weeks ago

Selected Answer: B

Whether a recipient receives a link-based experience or an inline experience depends on the recipient identity type: Microsoft 365 and Microsoft account recipients (for example, outlook.com users) get an inline experience in supported Outlook clients. All other recipient types, such as Gmail and Yahoo recipients, get a link-based experience.

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 37 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 37
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

You have a Microsoft 365 E5 subscription that contains the data loss prevention (DLP) policies shown in the following table.

Name	Applied to
DLP1	Microsoft Exchange Online email
DLP2	Microsoft SharePoint Online sites
DLP3	Microsoft Teams chat and channel messages

You have a custom employee information form named Template1.docx.

You plan to create a sensitive info type named Sensitive1 that will use the document fingerprint from Template1.docx.

What should you use to create Sensitive1, and in which DLP policies can you use Sensitive1? To answer, select the appropriate options in the answer area.

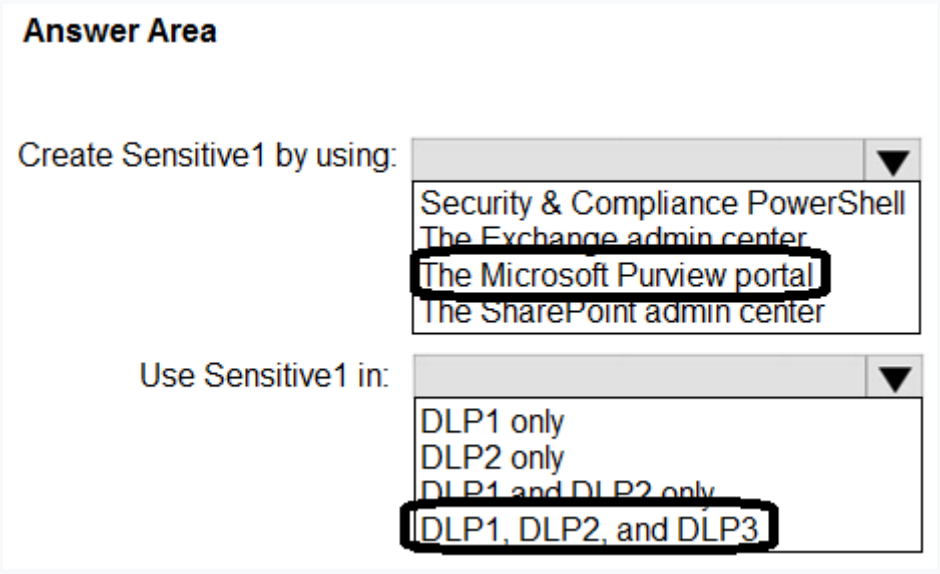
Answer Area

Create Sensitive1 by using:
- Security & Compliance PowerShell
- The Exchange admin center
- The Microsoft Purview portal
- The SharePoint admin center

Use Sensitive1 in:
- DLP1 only
- DLP2 only
- DLP1 and DLP2 only
- DLP1, DLP2, and DLP3

Hide Answer

Suggested Answer:



by Kamiles at *Aug. 25, 2025, 3:34 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

Purview portal
DLP 1, 2 & 3

To create your custom sensitive information type (SIT) named Sensitive1 using a document fingerprint from Template1.docx, you should use the Microsoft Purview portal and select Create sensitive info type from the Classifiers > Sensitive info types section, choosing the document fingerprint option to upload your template. You can then use the Sensitive1 SIT in any DLP policies within Microsoft Purview solutions that support custom SITs, such as those for Exchange Online, SharePoint Online, and Teams, to help protect sensitive information

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 38 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 38
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

You have a Microsoft 365 tenant that uses Microsoft Teams.

You create a data loss prevention (DLP) policy to prevent Microsoft Teams users from sharing sensitive information,

You need to identify which locations must be selected to meet the following requirements:

• Documents that contain sensitive information must not be shared inappropriately in Microsoft Teams.
• If a user attempts to share sensitive information during a Microsoft Teams chat session, the message must be deleted immediately.

Which three locations should you select? To answer, select the appropriate locations in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Location	Scope	Actions
☐ Exchange email	Turn on location to scope	
☐ SharePoint sites	Turn on location to scope	
☐ OneDrive accounts	Turn on location to scope	
☐ Teams chat and channel messages	Turn on location to scope	
☐ Instances	Turn on location to scope	
☐ On-premises repositories	Turn on location to scope	
☐ Fabric and Power BI workspaces	Turn on location to scope	

Hide Answer

Suggested Answer:

Answer Area

Location	Scope	Actions
☐ Exchange email	Turn on location to scope	
☐ SharePoint sites	Turn on location to scope	
☐ OneDrive accounts	Turn on location to scope	
☐ Teams chat and channel messages	Turn on location to scope	
☐ Instances	Turn on location to scope	
☐ On-premises repositories	Turn on location to scope	
☐ Fabric and Power BI workspaces	Turn on location to scope	

by Kamiles at *Aug. 25, 2025, 3:34 a.m.*

Comments

Eltooth Highly Voted 2 months, 3 weeks ago

Answer is correct.
SharePoint
OneDrive
Teams chat and channel messages

upvoted 6 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 39 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 39
Topic #: 1
[All SC-401 Questions]

You need to be alerted when users share sensitive documents from Microsoft OneDrive to any users outside your company.

What should you do?

A. From the Microsoft Defender portal create an activity policy.

B. From the Microsoft Purview portal start an Advanced eDiscovery search.

C. From the Exchange admin center, create a data loss prevention (DLP) policy.

D. From the Microsoft Defender portal, create a file policy. Most Voted

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (100%)

---

by Kamiles at *Aug. 25, 2025, 3:36 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

Selected Answer: D

D is correct answer.
From Defender portal, click Cloud Apps, Policy Management, Create Policy, File Policy

upvoted 3 times

Gtc_ 3 months, 1 week ago

Selected Answer: D

File policy.

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 40 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 40

Topic #: 1

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 subscription.

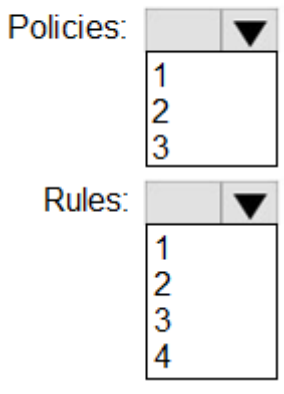
You identify the following data loss prevention (DLP) requirements:

- Send notifications to users if they attempt to send attachments that contain an EU Social Security Number (SSN) or Equivalent ID.
- Prevent any email messages that contain credit card numbers from being sent outside your organization.
- Block the external sharing of Microsoft OneDrive content that contains EU passport numbers.
- Send administrators email alerts if any rule matches occur.

What is the minimum number of DLP policies and rules you must create to meet the requirements? To answer, select the appropriate options in the answer area.

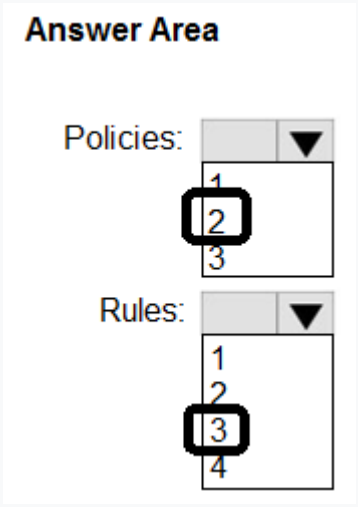
NOTE: Each correct selection is worth one point.

Answer Area



Hide Answer

Suggested Answer:



by Kamiles at *Aug. 25, 2025, 3:35 a.m.*

Comments

deeptha92 Highly Voted 3 months, 2 weeks ago

1 Policy and 3 rules in my opinion.

upvoted 8 times

Eltooth Most Recent 2 months, 2 weeks ago

✅ Needs a rule that detects EU SSN or equivalent ID and sends a user notification.
✅ Needs a rule that blocks external email with credit card numbers.
✅ Needs a rule scoped to OneDrive that blocks external sharing when EU passport numbers are detected.
✅ This is a notification setting that can be applied across all rules in a policy.
✅ Minimum Number of Policies and Rules
You can combine multiple rules into a single DLP policy if they apply to different locations (e.g., Exchange, OneDrive) and have different actions.
However, Exchange Online and OneDrive require separate policies because DLP policies are scoped by location.
So: Policy 1: For Exchange Online
Rule 1: Notify users for EU SSN or Equivalent ID
Rule 2: Block external email with credit card numbers
Admin alert setting applies to both rules
Policy 2: For OneDrive
Rule 3: Block external sharing for EU passport numbers
Admin alert setting applies to this rule
✅ Final Answer:
Minimum Policies: 2
Minimum Rules: 3

upvoted 4 times

Caezarlay 2 months, 2 weeks ago

Given answer is correct.
1 policy for email with 2 rules including alert
1 policy for OneDrive with 1 rule including alert

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 41 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 41

Topic #: 1

[All SC-401 Questions]

You have a Microsoft OneDrive folder that contains the files shown in the following table.

Type	Number of files
.jpg	50
.docx	300
.txt	50
.zip	20

In Microsoft Defender for Cloud Apps, you create a file policy to automatically apply a classification.

What is the effect of applying the policy?

A. The policy will apply to only the .docx and .txt files. The policy will classify the files immediately.

B. The policy will apply to only the .docx files. The policy will classify only 100 files daily.

C. The policy will apply to all the files. The policy will classify only 100 files daily.

D. The policy will apply to only the .docx and .txt files. The policy will classify the files within 24 hours. Most Voted

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (55%) C (45%)

by Kamiles at *Aug. 25, 2025, 3:35 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

Selected Answer: D

All files in example (except .jpg) are supported.
There is no official 100 file daily limit either.
No answer is correct but be aware of DfCA supported file types.
https://learn.microsoft.com/en-us/defender-cloud-apps/data-protection-policies#supported-file-types

upvoted 2 times

Nurob 3 months, 1 week ago

Selected Answer: D

Images files are not supported in MDCA, also the 100 files a day limit is Auto-Labelling limitation not MDCA. Based on that table only Docx and Text File should be automatically classified.. https://learn.microsoft.com/en-us/defender-cloud-apps/data-protection-policies?utm_source=chatgpt.com#supported-file-types

upvoted 4 times

Suranka 3 months, 2 weeks ago

Selected Answer: C

Google answer

upvoted 1 times

Suranka 3 months, 2 weeks ago

Correction: My answer is B (You can only apply automatic classification to .docx files using Defender for Cloud Apps. The other file types (.jpg, .txt, .zip) are not supported for this feature.)

upvoted 4 times

deeptha92 3 months, 2 weeks ago

Selected Answer: C

Defender for Cloud Apps engines perform content inspection by extracting text from (100+) common file types including Office, Open Office, compressed files, various rich text formats, XML, HTML, and more.

upvoted 3 times

deeptha92 3 months, 2 weeks ago

Selected Answer: C

Defender for Cloud Apps engines perform content inspection by extracting text from (100+) common file types including Office, Open Office, compressed files, various rich text formats, XML, HTML, and more.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 42 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 42
Topic #: 1
[All SC-401 Questions]

You have a Microsoft 365 E5 subscription.

You plan to deploy Microsoft Purview Data Security Posture Management for AI (OSPM for AI) to protect company data that contains Personally Identifiable Information (PII) from being shared with third-party generative AI tools.

You need to complete the prerequisites for the planned deployment.

Which two Microsoft Purview solutions should you use? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Data Loss Prevention Most Voted
B. Information Barriers
C. Insider Risk Management
D. Communication Compliance
E. Audit Most Voted

Hide Answer

Suggested Answer: *AE*

Community vote distribution

AC (44%) AE (44%) 13%

by Kamiles at *Aug. 25, 2025, 3:34 a.m.*

Comments

Leon1969 Highly Voted 1 month, 4 weeks ago

Selected Answer: AE

A: DLP is required to prevent sensitive information from being shared:
E: Because this is a prerequisite for DSMP for AI

upvoted 6 times

Said_kram Most Recent 3 weeks, 2 days ago

Selected Answer: AE

IRM only for third-site AI monitoring, so DLP + Audit seems ok for me.

upvoted 1 times

Caezarlay 2 months, 2 weeks ago

Selected Answer: AC

Required for monitoring interactions with third-party generative AI sites:

Devices are onboarded to Microsoft Purview, required for:

Gaining visibility into sensitive information that's shared with third-party generative AI sites. For example, a user pastes credit card numbers into ChatGPT.
Applying endpoint DLP policies to warn or block users from sharing sensitive information with third-party generative AI sites. For example, a user identified as elevated risk in Adaptive Protection is blocked with the option to override when they paste credit card numbers into ChatGPT.
The Microsoft Purview browser extension is deployed to Windows users and required to discover visits to third-party generative AI sites by using an Insider Risk Management policy. The browser extension is also required for endpoint DLP policies on Windows when you use Chrome.

https://learn.microsoft.com/en-us/purview/dspm-for-ai-considerations

upvoted 3 times

ea256cf 2 months, 2 weeks ago

Selected Answer: AC

A and C

upvoted 3 times

Eltooth 2 months, 3 weeks ago

Selected Answer: AC

DLP & IRM.
To complete the prerequisites:
✅ A. Data Loss Prevention
Why: DLP policies are essential for detecting and preventing the sharing of sensitive data like PII. They allow you to define rules that block or monitor data movement to unauthorised destinations, including generative AI platforms.
✅ C. Insider Risk Management
Why: Insider Risk Management helps identify and mitigate risky user behaviour, such as attempts to share sensitive data externally or with AI tools. It provides visibility into potential data exfiltration and supports proactive controls.
FYI - Audit must be enabled first and devices onboarded into Purview.

upvoted 1 times

deeptha92 3 months, 2 weeks ago

Selected Answer: AD

https://learn.microsoft.com/en-us/purview/dspm-for-ai-considerations

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 43 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 43
Topic #: 1
[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that contains four users named User1, User2, User3, and User4 and a file named File1.docx. File1 has a sensitivity label applied. The label is configured as shown in the following table.

User	Permission
User1	Owner
User2	Editor
User3	Restricted Editor
User4	Viewer

Which users can summarize File1 by using Microsoft 365 Copilot?

A. User1 only
B. User1 and User2 only Most Voted
C. User1, User2, and User3 only
D. User1, User2, User3, and User4

Hide Answer

Suggested Answer: *B*

Community vote distribution
B (100%)

by Kamiles at *Aug. 25, 2025, 3:34 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

Selected Answer: B

B is the correct answer.

upvoted 2 times

deeptha92 3 months, 2 weeks ago

Selected Answer: B

Sensitivity labels work with Microsoft 365 Copilot by restricting access to sensitive information based on user permissions. Copilot can only access and summarize data for which the user has "View" and "Extract" rights, as defined by sensitivity labels and their encryption settings

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 44 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 44
Topic #: 1
[All SC-401 Questions]

You have a Microsoft 365 E5 subscription. The subscription contains a user named User1 and the sensitivity labels shown in the following table.

Name	Authenticated users: View content (VIEW)	Authenticated users: Copy and extract content (EXTRACT)	Authenticated users: Export content (EXPORT)
Label1	Granted	Not granted	Not granted
Label2	Granted	Granted	Not granted
Label3	Granted	Not granted	Granted

You publish the labels to User1.

The subscription contains the files shown in the following table.

Name	Label
File1	Label1
File2	Label2
File3	Label3

Which files can Microsoft 365 Copilot summarize for User1?

A. File2 only Most Voted

B. File3 only

C. File2 and File3 only

D. File1, File2, and File3

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (91%) 9%

by Kamiles at *Aug. 25, 2025, 3:34 a.m.*

Comments

florinvele Highly Voted 2 months, 4 weeks ago

Selected Answer: A

In the Microsoft Purview portal, the EXTRACT usage right is displayed as Copy and extract content(EXTRACT)
https://learn.microsoft.com/en-us/purview/ai-m365-copilot-considerations#copilot-honors-existing-protection-with-the-extract-usage-right

upvoted 6 times

Nurob Most Recent 3 months, 1 week ago

Selected Answer: A

View and extract oemrissions are required to be able to summarize

upvoted 2 times

Gtc_ 3 months, 2 weeks ago

Selected Answer: A

Need Extract enabled for Copilot.

https://learn.microsoft.com/en-us/purview/ai-m365-copilot-considerations#copilot-honors-existing-protection-with-the-extract-usage-right

upvoted 2 times

Suranka 3 months, 2 weeks ago

Selected Answer: C

Google answer

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 45 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 45

Topic #: 1

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.

You need to ensure that you receive an alert when a user uploads a document to a third-party cloud storage service.

What should you use?

A. an insider risk policy

B. a file policy

C. a sensitivity label

D. an activity policy Most Voted

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (71%) B (29%)

by 454252dfr at *Aug. 22, 2025, 3:42 p.m.*

Comments

mlstud 5 days, 3 hours ago

Selected Answer: D

To receive an alert when a user uploads a document to a third-party cloud storage service using Microsoft Defender for Cloud Apps, you should create an Activity Policy.

upvoted 1 times

f2b34cb 1 month ago

Selected Answer: B

You should use a file policy in Microsoft Defender for Cloud Apps to create an alert for uploads to third-party cloud storage services. By creating a file policy, you can specify conditions, such as when a file is uploaded to a third-party service, and set a severity level to trigger an alert.

upvoted 2 times

Suranka 3 months, 2 weeks ago

Selected Answer: D

Activity policy

Designed to detect specific user activities in apps (e.g., upload, download, share).

Can generate alerts when a user uploads a document to an unsanctioned or third-party cloud storage app.

upvoted 1 times

454252dfr 3 months, 3 weeks ago

Selected Answer: D

Correct answer: D. an activity policy

An activity policy in Microsoft Defender for Cloud Apps lets you monitor and get alerts on specific user actions, such as uploading a document to a third-party cloud storage service. Other options (insider risk, file policy, sensitivity label) focus on data classification, protection, or insider threats, but they do not trigger alerts based on user activities.

upvoted 3 times

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 46 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 46

Topic #: 1

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that uses Microsoft Purview.

You are evaluating the use of custom data assessment scans to identify the potential oversharing of data in the subscription.

What is the maximum number of items the data assessments can support per location?

A. 50,000

B. 100,000

C. 200,000 Most Voted

D. 500,000

Hide Answer

Suggested Answer: *C*

Community vote distribution

C (78%) D (22%)

by Kamiles at *Aug. 25, 2025, 3:33 a.m.*

Comments

Lapiduse 2 months ago

Selected Answer: C

Data risk assessments currently support a maximum of 200,000 items per location. The count of files reported might not be accurate when there are more than 100,000 files per location.

upvoted 1 times

Nurob 3 months, 1 week ago

Selected Answer: C

Good call from GTC_ with the article
https://learn.microsoft.com/en-us/purview/dspm-for-ai

upvoted 2 times

JohnyBest 3 months, 1 week ago

Selected Answer: C

Documentation of DSPM (Data Security Posture Management for AI)

upvoted 2 times

Gtc_ 3 months, 2 weeks ago

Selected Answer: C

This data risk assessment is created in the Custom assessments category. Wait for the status of your assessment to display Scan completed, and select it to view details. To rerun a custom data risk assessment, and to see results after the 30-day expiration, use the duplicate option to create a new assessment, starting with the same selections.

Both the default and custom data risk assessments provide an Export option that let you save and customize the data into a choice of file formats (Excel, .csv, JSON, TSV).

Data risk assessments currently support a maximum of 200,000 items per location. The count of files reported might not be accurate when there are more than 100,000 files per location.

https://learn.microsoft.com/en-us/purview/dspm-for-ai

This is the only figure for actual items within the documentation.

upvoted 2 times

Suranka 3 months, 2 weeks ago

Selected Answer: D

As of July 30, 2025, the maximum number of items per location that custom data assessment scans support in Microsoft Purview for a Microsoft 365 E5 subscription is 500,000.
This limit is specified within the eDiscovery limits documentation on Microsoft Learn, where it lists a limit of 500,000 total locations and 500,000 exported results (items) for search actions. Custom data assessments, which are a type of data scan and search, operate within these documented limits.
You also mention that counts may become inaccurate above 100,000 items, and while this has been noted in the past, Microsoft's official documentation continues to list the supported limit for exportable items at 500,000. This suggests that the platform is capable of processing up to this higher number, but the reported inaccuracy is a good practice point for interpreting the scan results on extremely large location

upvoted 1 times

Gtc_ 3 months, 2 weeks ago

This isn't related to eDiscovery. Below are eDiscovery figures that relate to cases, not assessments.

https://learn.microsoft.com/en-us/purview/edisc-ref-limits

upvoted 2 times

cncpower 3 months, 2 weeks ago

Selected Answer: D

Microsoft Purview can support per location is 500,000.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 47 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 47

Topic #: 1

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 365 E5 subscription.

You plan to create a new sensitive information type (SIT) by using the Microsoft Purview portal.

You need to copy and modify an existing SIT from which to create the new SIT.

What are two SITs that you can copy and modify? To answer, select the appropriate SITs in the answer area.

NOTE: Each correct selection is worth one point.

Hide Answer

Suggested Answer:

by Kamiles at *Aug. 25, 2025, 3:36 a.m.*

Comments

Ender3 2 months, 1 week ago

I believe the correct answers are:
ABA Routing Number (Entity)
Adatum numbers (Entity)

All Credential Types and All Full Names cannot be copied. I tried. Please correct the official answers.

upvoted 3 times

Eltooth 2 months, 2 weeks ago

Entities are only able to be copied.
ABA Routing and Adatum are only options.

upvoted 3 times

Gtc_ 3 months, 2 weeks ago

ABA Routing and Adatum is correct. Only repeatable, standardized patterns can be copied.

https://learn.microsoft.com/en-us/purview/sit-common-scenarios?utm_source=chatgpt.com

https://learn.microsoft.com/en-us/purview/sit-create-a-custom-sensitive-information-type

upvoted 4 times

deeptha92 3 months, 2 weeks ago

ABA Routing Number and Adatum Number

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 48 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 48

Topic #: 1

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that has a Microsoft Purview exact data match (EDM) classifier named EDM1.

You plan to create the Microsoft Purview policies shown in the following table.

Name	Type
DLP1	Data loss prevention (DLP)
Insider1	Insider risk management
Retention1	Retention

Which policies can use EDM1?

A. DLP1 only

B. Retention1 only

C. DLP1 and Insider1 only Most Voted

D. Insider1 and Retention1 only

E. DLP1, Insider1, and Retention1

Hide Answer

Suggested Answer: *C*

Community vote distribution

C (91%) 9%

by Kamiles at *Aug. 25, 2025, 3:33 a.m.*

Comments

deeptha92 Highly Voted 3 months, 2 weeks ago

Selected Answer: C

EDM SITs can be used in:

Microsoft Purview Data Loss Prevention
Auto-labeling (service and client side)
Microsoft Purview Insider Risk Management policies
Microsoft Purview eDiscovery

Microsoft Purview Insider Risk Management
Microsoft Defender for Cloud Apps

upvoted 9 times

mlstud Most Recent 5 days, 3 hours ago

Selected Answer: C

Retention policies in Microsoft Purview do not support EDM-based SITs as conditions

upvoted 1 times

tila_s 3 months ago

Selected Answer: A

EDM SITs can be used in:

Microsoft Purview DLP

Auto-labeling (service side only)

Microsoft Defender for Cloud Apps

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 49 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 49

Topic #: 1

[All SC-401 Questions]

You have a Microsoft 365 tenant.

You create the following:

• A sensitivity label
• An auto-labeling policy

You need to ensure that the sensitivity label is applied to all the data discovered by the auto-labeling policy.

What should you do first?

A. Run the Enable-TransportRule cmdlet.

B. Enable insider risk management.

C. Create a trainable classifier

D. Run the policy in simulation mode. Most Voted

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (100%)

by Kamiles at *Aug. 25, 2025, 3:33 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: D

D is correct answer: Run policy in simulation mode.

upvoted 3 times

Lapiduse 2 months, 3 weeks ago

Selected Answer: D

Simulation mode

upvoted 2 times

Gtc_ 3 months, 2 weeks ago

Selected Answer: D

Simulation mode after creating the items is the best way to see whether or not the policy is adequately being adhered to.

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 51 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 51

Topic #: 1

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that uses Microsoft Teams.

You plan to implement sensitivity labels.

You need to ensure that you can view and apply sensitivity labels to new Microsoft Teams sites.

What should you do first?

A. Run the Set-SPOSite cmdlet.

B. Create a new sensitivity label scoped to Groups & sites.

C. Configure the EnableMIPLabels setting in Microsoft Entra ID. Most Voted

D. Run the Execute-AzureAdLabelSync cmdlet.

Hide Answer

Suggested Answer: *C*

Community vote distribution

C (100%)

by Kamiles at *Aug. 25, 2025, 3:35 a.m.*

Comments

deeptha92 Highly Voted 3 months, 2 weeks ago

Selected Answer: C

To use sensitivity labels for Teams/Groups/Sites (container labels) you must first enable them in Entra ID (EnableMIPLabels). After that, create a label scoped to Groups & sites and publish it; you can optionally run Execute-AzureAdLabelSync to speed up sync. Set-SPOSite isn't needed for new Teams sites.

upvoted 6 times

Eltooth Most Recent 2 months, 2 weeks ago

Selected Answer: C

C is correct answer.
https://learn.microsoft.com/en-us/entra/identity/users/groups-assign-sensitivity-labels?tabs=microsoft

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 52 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 52
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Type	Primary email address
Group1	Microsoft 365	Group1@contoso.com
Dist1	Distribution	Dist1@contoso.com

The subscription contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Dist1
User3	*None*

You create the mail flow rules shown in the following table.

Name	Apply this rule if	Do the following
Rule1	The recipient is a member of group1@contoso.com	Apply Office 365 Message Encryption and rights protection
Rule2	The sender is dist1@contoso.com	Apply Office 365 Message Encryption and rights protection

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If User2 sends an email message to User3, the message is encrypted automatically.	○	○
If User2 sends an email message to User1, the message is encrypted automatically.	○	○
If User3 sends an email message to Group1, the message delivered to User1 is encrypted automatically.	○	○

Hide Answer

Suggested Answer:

Answer Area

Statements	Yes	No
If User2 sends an email message to User3, the message is encrypted automatically.	○	○
If User2 sends an email message to User1, the message is encrypted automatically.	○	○
If User3 sends an email message to Group1, the message delivered to User1 is encrypted automatically.	○	○

by Kamiles at *Aug. 25, 2025, 3:33 a.m.*

Comments

florinvele Highly Voted 2 months, 4 weeks ago

NO / YES / NO
First statement is NO because User3 is not a member of group1 (Rule1) and Rule2 says "If the sender is dist1 - so sending as the Dist1.
upvoted 6 times

bobg 2 weeks, 4 days ago

just because you are in a distribution group doesnt mean your own primary email address changes though? I think it's N, N, N.
upvoted 1 times

Ender3 Most Recent 2 months ago

No, Yes, No
The 3rd statement is a bit tricky, but no rules should apply because the message is sent to Group1's mailbox not to any member of the group (not a match for Rule1). Encryption occurs during transport processing to Group1, any member seeing the message after delivery sees an unencrypted message.
upvoted 1 times

Eltooth 2 months, 2 weeks ago

No
Yes
Yes - User 1 is a recipient Of Group1
upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 53 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 53

Topic #: 1

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that has a sensitivity label named Sensitivity1.

You plan to create an auto-labeling policy that will apply Sensitivity1 to Microsoft Exchange Online mailboxes.

On February 1, you create the auto-labeling policy and enable simulation mode by using the default settings. No modifications are made to the policy in simulation mode.

When will the policy first be turned on?

A. February 2

B. February 6

C. February 15

D. never Most Voted

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (100%)

by Kamiles at *Aug. 25, 2025, 3:35 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: D

D is correct answer. No auto-enabling of policy from simulation mode.

upvoted 1 times

Lapiduse 2 months, 3 weeks ago

Selected Answer: D

https://learn.microsoft.com/en-us/purview/apply-sensitivity-label-automatically
For the Decide if you want to test out the policy now or later page: Select Run policy in simulation mode if you're ready to run the auto-labeling policy now, in simulation mode. Then decide whether to automatically turn on the policy if it's not edited for 7 days (NOT ENABLED BY DEFAULT)

upvoted 3 times

Gtc_ 3 months, 2 weeks ago

Selected Answer: D

Simulation mode doesn't enable the policy.

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 54 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 54

Topic #: 1

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription.

You need to ensure that any message or document containing a credit card number is deleted automatically 12 months after it was created. The solution must minimize administrative effort.

Which two components should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. an auto-labeling policy for a sensitivity label

B. a sensitivity label

C. an auto-labeling policy for a retention label Most Voted

D. a retention label Most Voted

E. a sensitive information type (SIT)

Hide Answer

Suggested Answer: *CD*

Community vote distribution

CD (100%)

by Kamiles at *Aug. 25, 2025, 3:35 a.m.*

Comments

deeptha92 Highly Voted 3 months, 2 weeks ago

Selected Answer: CD

1. Create a retention label that retains and delete contents after 12 months
2. Create an Auto Labeling policy "Auto Apply Label" for a retention label

upvoted 5 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 56 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 56
Topic #: 1
[All SC-401 Questions]

SIMULATION
-

Username and password
-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and select the username below.

To enter your password, place your cursor in the Enter password box and select the password below.

Microsoft 365 Username:
admin@WWLx971455.onmicrosoft.com

Microsoft 365 Password: XXXXXXXXX

If the Microsoft Edge browser or Microsoft 365 portal does not load successfully, select the Microsoft Edge browser icon from the task bar, type the URL “https://admin microsoft.com”, and press Enter.

The following information is for technical support purposes only:
Lab Instance: XXXXXXXX.

Task 2
-

You discover that all users can apply the Confidential – Finance label.

You need to ensure that the Confidential – Finance label is available only to the members of the Leadership group.

Hide Answer

Suggested Answer:

Assign sensitivity labels to Microsoft 365 groups in Microsoft Entra ID
Microsoft Entra ID supports applying sensitivity labels published by the Microsoft Purview compliance portal to Microsoft 365 groups. Sensitivity labels apply to groups across services like Outlook, Microsoft Teams, and SharePoint. F

Assign a label to an existing group in the Microsoft Entra admin center

Step 1: Sign in to the Microsoft Entra admin center as at least a Global Administrator.

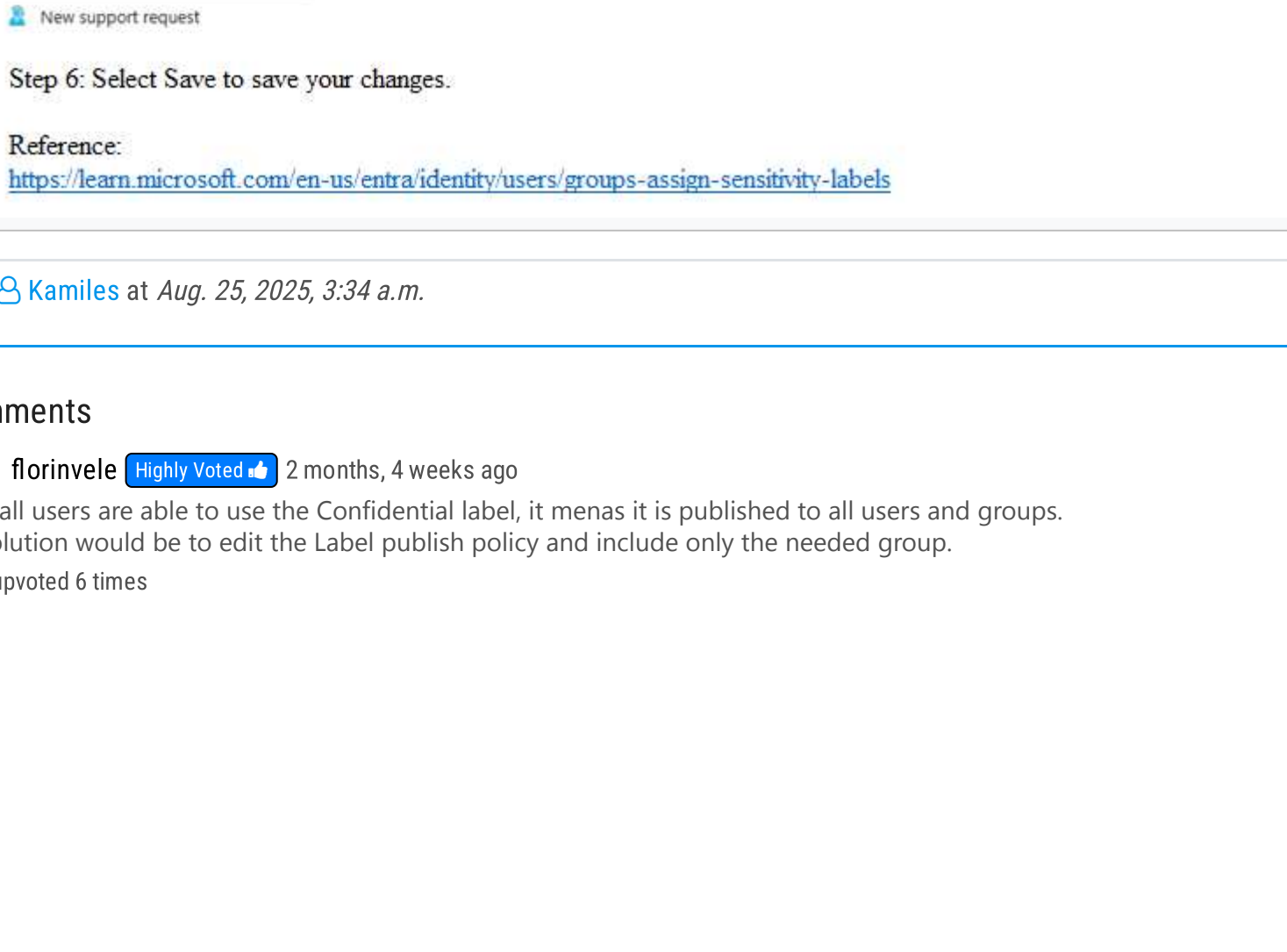
Step 2: Select Microsoft Entra ID.

Step 3: Select Groups

Step 4: From the All groups page, select the group that you want to label.

Step 5: On the selected group's page, select Properties and select a sensitivity label from the list.

Select the Confidential - Finance label



Step 6: Select Save to save your changes.

Reference:
https://learn.microsoft.com/en-us/entra/identity/users/groups-assign-sensitivity-labels

by Kamiles at *Aug. 25, 2025, 3:34 a.m.*

Comments

florinvele Highly Voted 2 months, 4 weeks ago

If all users are able to use the Confidential label, it menas it is published to all users and groups. solution would be to edit the Label publish policy and include only the needed group.

upvoted 6 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 59 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 59
Topic #: 1
[All SC-401 Questions]

You have a Microsoft 365 E5 subscriptions.

You deploy Microsoft Purview Data Security Posture Management for AI (OSPM for AI).

You need to edit the default policies created as part of the deployment.

Which two Microsoft Purview solutions should you use? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Insider Risk Management Most Voted
B. Information Protection
C. Compliance Manager
D. DSPM for AI
E. Information Barriers
F. Data Lifecycle Management
G. Data Loss Prevention Most Voted

Hide Answer

Suggested Answer: *AG*

Community vote distribution

AG (100%)

by Kamiles at *Aug. 25, 2025, 3:33 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: AG

A and G are correct.
DSPM for AI policies link (Edit policy in solution) takes you back to IRM policies.

upvoted 2 times

Lapiduse 2 months, 3 weeks ago

Selected Answer: AG

https://learn.microsoft.com/en-us/purview/dspm-for-ai-considerations#default-policies-for-data-discovery-using-data-security-posture-management-for-ai

upvoted 2 times

florinvele 2 months, 4 weeks ago

Selected Answer: AG

https://learn.microsoft.com/en-us/purview/dspm-for-ai-considerations#default-policies-for-data-discovery-using-data-security-posture-management-for-ai

upvoted 4 times

Gtc_ 3 months, 2 weeks ago

Selected Answer: AG

I feel like there are multiple correct combinations, but DLP and IRM are listed explicitly in the docs.

https://learn.microsoft.com/en-us/purview/dspm-for-ai-considerations

upvoted 4 times

Suranka 3 months, 2 weeks ago

Selected Answer: AG

B. Information Protection
Some default policies create sensitivity labels and sensitivity label policies.
You must navigate to the Information Protection solution in the Purview portal to view and edit these labels and their associated policies.
G. Data Loss Prevention (DLP)
Many of the default "one-click" policies for DSPM for AI are, in fact, DLP policies.
These policies detect or block the sharing of sensitive information with AI applications.
To modify the rules, conditions, or actions of these policies, you must use the Data Loss Prevention solution in the Purview portal.

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 60 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 60
Topic #: 1
[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that contains thee users named User1, User2, and User3 and a file named File1.docx.

You create a sensitivity label named Label1 as shown in the following exhibit.

Assign permissions to specific users and groups *

Assign permissions

3 items

Users and groups	Permissions	Edit	Delete
User1@86s40q.onmicrosoft.com	Co-Author		
User2@86s40q.onmicrosoft.com	Review		
User3@86s40q.onmicrosoft.com	Viewer		

☐ Use dynamic watermarking

☑ Use Double Key Encryption

You apply Label1 to File1.

For which users can Microsoft 365 Copilot summarize File1?

A. No user Most Voted

B. User1 only

C. User1 and User2 only

D. User1, User2, and User3

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (100%)

by 454252dfr at *Aug. 22, 2025, 4:19 p.m.*

Comments

deeptha92 Highly Voted 3 months, 2 weeks ago

Selected Answer: A

Because Double Key Encryption (DKE) is intended for your most sensitive data that is subject to the strictest protection requirements, Copilot and agents can't access this data. As a result, items protected by DKE won't be returned by Copilot, and if a DKE item is open (data in use), you won't be able to use Copilot in the app

https://learn.microsoft.com/en-us/purview/ai-m365-copilot-considerations#information-protection-considerations-for-microsoft-365-copilot

upvoted 6 times

Eltooth Most Recent 2 months, 2 weeks ago

Selected Answer: A

A is correct answer: DKE

upvoted 1 times

Lapiduse 2 months, 3 weeks ago

Selected Answer: A

Because of DKE

upvoted 1 times

454252dfr 3 months, 3 weeks ago

Selected Answer: A

The correct answer is A. No user
User1 (Co-Author) → Can open/edit the file, but Copilot cannot summarize due to DKE.
User2 (Review) → Can review the file, but Copilot cannot summarize due to DKE.
User3 (Viewer) → Can view the file, but Copilot cannot summarize due to DKE.

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 61 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 61
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

You have a Microsoft 365 E5 subscription that contains four users named User1, User2, User3, and User4 and a file named File1.docx.

To File1, you apply a sensitivity label that has the permissions shown in the following exhibit.

Assign permissions to specific users and groups *

Assign permissions

4 items

Users and groups	Permissions	Edit	Delete
User1@86s40q.onmicrosoft.com	Co-Owner		
User2@86s40q.onmicrosoft.com	Co-Author		
User3@86s40q.onmicrosoft.com	Reviewer		
User4@86s40q.onmicrosoft.com	Viewer		

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

Microsoft 365 Copilot can summarize File1 for **[answer choice]**.

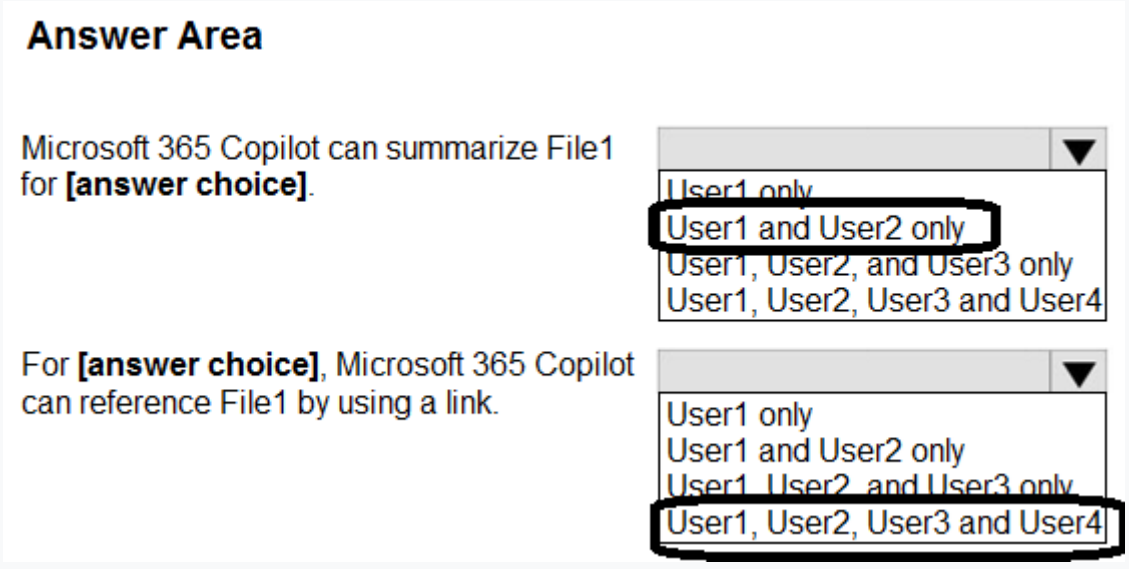
- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3 and User4

For **[answer choice]**, Microsoft 365 Copilot can reference File1 by using a link.

- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3 and User4

Hide Answer

Suggested Answer:


Answer Area
Microsoft 365 Copilot can summarize File1 for [answer choice].
User1 only
User1 and User2 only
User1, User2, and User3 only
User1, User2, User3 and User4
For [answer choice], Microsoft 365 Copilot can reference File1 by using a link.
User1 only
User1 and User2 only
User1, User2, and User3 only
User1, User2, User3 and User4

by Kamiles at *Aug. 25, 2025, 3:33 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Answer looks correct.
User 1 & 2 can summarise.
User 1, 2, 3 & 4 can reference by link.

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 62 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 62
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

You have a Microsoft 365 E5 subscription that uses Microsoft Purview Audit (Premium) with the 10-Year Audit Log Retention add-on license.

The subscription contains the audit retention policies shown in the following table.

Name	Users	Record type	Activities	Duration	Priority
RP1	User1	SharePoint	Created site collection	1 Year	30
RP2	User1	SharePoint	*None*	3 Years	20
RP3	User1	SharePoint	Created site collection	3 Years	40
RP4	User1	SharePoint	Renamed site	6 Months	10

From the SharePoint Online admin center, User1 performs the actions shown in the following table.

Name	Description
Action1	Archives a site
Action2	Creates a site collection
Action3	Renames a site

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

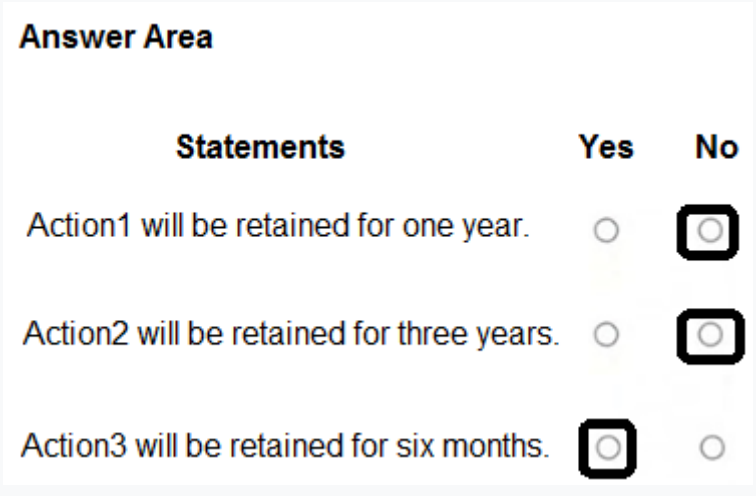
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Action1 will be retained for one year.	○	○
Action2 will be retained for three years.	○	○
Action3 will be retained for six months.	○	○

Hide Answer

Suggested Answer:



by Kamiles at *Aug. 25, 2025, 3:32 a.m.*

Comments

florinvele Highly Voted 2 months, 4 weeks ago

NO - Action1 is retained 3 years based on RP2 (RP4 has highest prio but does not include the action mentioned)
YES - Action2 is retained 3 years based on RP2
YES - Action3 is retained 6 months based on RP4 (highest prio)

upvoted 9 times

Alcpt Most Recent 3 weeks, 1 day ago

N - RP2
N - RP1 (priority 30) dont get caught by RP3 which has priority of 40!
Y - RP4

upvoted 1 times

Alcpt 3 weeks ago

first answer is wrong, heres my update:
act1 = RP2 = No,
act2 = RP3 = yes,
act3 = RP2 = no, (remember that RP2 has higher priority than RP4 and is "none" = "all actions")

upvoted 2 times

Alcpt 1 week, 2 days ago

N Y Y as per florinvele

upvoted 2 times

Ender3 2 months ago

I could not find any evidence that when there is overlapping scope between two audit retention policies, the longer duration wins regardless of priority. I know this principle applies to records retention but if it were applicable here it would have been explicitly stated somewhere. The materials only state that a policy with a higher priority (lower number) takes precedence here: https://learn.microsoft.com/en-us/purview/audit-log-retention-policies. Based on that, my answers are as follows:
1. No. Since there is no retention policy specific to the "Archives a site" activity, RP2 applies, so retention should be 3 years, not 1.
2. No. RP1 and RP3 apply to "Create site collection" activity, and since RP1 has a higher priority, it takes effect, and the retention shall be 1 year, not 3.
3. Yes. Only RP4 is specific to the "Renamed site" activity, so 6 months is correct.

upvoted 3 times

Eltooth 2 months, 2 weeks ago

No
Yes
No - the 1 year retention takes precedence over the 6 month.

When multiple retention policies apply to the same content—such as a SharePoint site or Microsoft 365 group—the longest retention period always wins. This is a core principle of Microsoft Purview's retention engine.

So in your case:

If a 1-year and a 6-month retention policy are both applied to the same site,
The 1-year policy will take precedence.
This ensures that content is not deleted prematurely if any policy requires it to be retained longer.

upvoted 1 times

Gtc_ 3 months, 2 weeks ago

No, Yes, No

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 63 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 63
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

You have a Microsoft 365 E5 subscription that contains two Windows devices named Device1 and Device2. Device1 has the default browser set to Microsoft Edge. Device2 has the default browser set to Google Chrome.

You need to ensure that Microsoft Purview insider risk management can collect signals when a user copies files to a USB device by using their default browser.

What should you deploy to each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

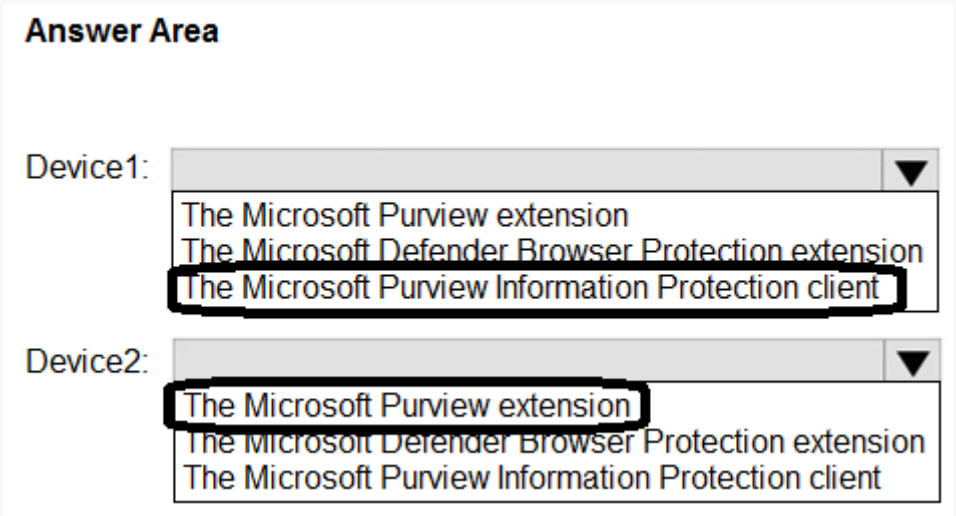
Answer Area

Device1:
- The Microsoft Purview extension
- The Microsoft Defender Browser Protection extension
- The Microsoft Purview Information Protection client

Device2:
- The Microsoft Purview extension
- The Microsoft Defender Browser Protection extension
- The Microsoft Purview Information Protection client

Hide Answer

Suggested Answer:


Answer Area
Device1:
The Microsoft Purview extension
The Microsoft Defender Browser Protection extension
The Microsoft Purview Information Protection client
Device2:
The Microsoft Purview extension
The Microsoft Defender Browser Protection extension
The Microsoft Purview Information Protection client

by Kamiles at *Aug. 25, 2025, 3:33 a.m.*

Comments

Ender3 Highly Voted 2 months ago

MS Purview Extension for both devices

upvoted 6 times

Caezarlay Highly Voted 2 months, 2 weeks ago

Device1 (Edge): The Microsoft Purview extension
Device2 (Chrome): The Microsoft Purview extension

upvoted 6 times

Eltooth Most Recent 2 months, 2 weeks ago

Device 1 - Information Protection client
Device 2 - Purview extension

upvoted 1 times

Gtc_ 3 months, 2 weeks ago

Agree with answer

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 64 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 64
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

You have a Microsoft 365 E5 tenant.

You have sensitivity labels as shown in the Sensitivity Labels exhibit. (Click the Sensitivity Labels tab.)

The Confidential/External sensitivity label is configured to encrypt files and emails when applied to content.

The sensitivity labels are published as shown in the Published exhibit. (Click the Published tab.)

Sensitivity Policy1

Edit policy | Delete policy

Name
Sensitivity Policy1

Description

Published labels
Public
General
Confidential
Confidential/External
Confidential/Internal

Published to
All

Policy settings
Users must provide justification to remove a label or lower its classification

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
The Internal sensitivity label inherits all the settings from the Confidential label.	○	○
Users must provide justification if they change the label of content from Confidential/Internal to Confidential/External.	○	○
Content that has the Confidential/External label applied will retain the encryption settings if the sensitivity label is removed from the label policy.	○	○

Hide Answer

Suggested Answer:

Answer Area

Statements	Yes	No
The Internal sensitivity label inherits all the settings from the Confidential label.	○	●
Users must provide justification if they change the label of content from Confidential/Internal to Confidential/External.	●	○
Content that has the Confidential/External label applied will retain the encryption settings if the sensitivity label is removed from the label policy.	●	○

by 454252dfr at *Aug. 22, 2025, 4:30 p.m.*

Comments

454252dfr Highly Voted 3 months, 3 weeks ago
Incorrect. NO, NO, YES
upvoted 17 times

msuan Highly Voted 2 months, 3 weeks ago

NO NO YES agree

upvoted 5 times

Ender3 Most Recent 2 months ago

No, sublabels do not inherit from their parent label, all settings must be configured.
No, going from higher to lower priority does not require a justification.
Yes, the label is already applied and it's with the file.

upvoted 2 times

Eltooth 2 months, 2 weeks ago

No
No
Yes

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 65 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 65
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

You have a Microsoft SharePoint Online site named Site1 and a sensitivity label named Sensitivity1. Sensitivity1 adds a watermark and a header to content.

You create a policy to automatically apply Sensitivity1 to emails in Microsoft Exchange Online and Site.

How will Sensitivity1 mark matching emails and Site1 documents? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Exchange Online email:
- A header only
- A watermark only
- A watermark and a header

Site1 documents:
- A header only
- A watermark only
- A watermark and a header

Show Suggested Answer

by Kamiles at *Aug. 25, 2025, 3:36 a.m.*

Comments

Eltooth 2 months, 2 weeks ago
Header only
Watermark and a header
upvoted 2 times

Gtc_ 3 months, 2 weeks ago
Given is correct.
upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam

Go to Exam

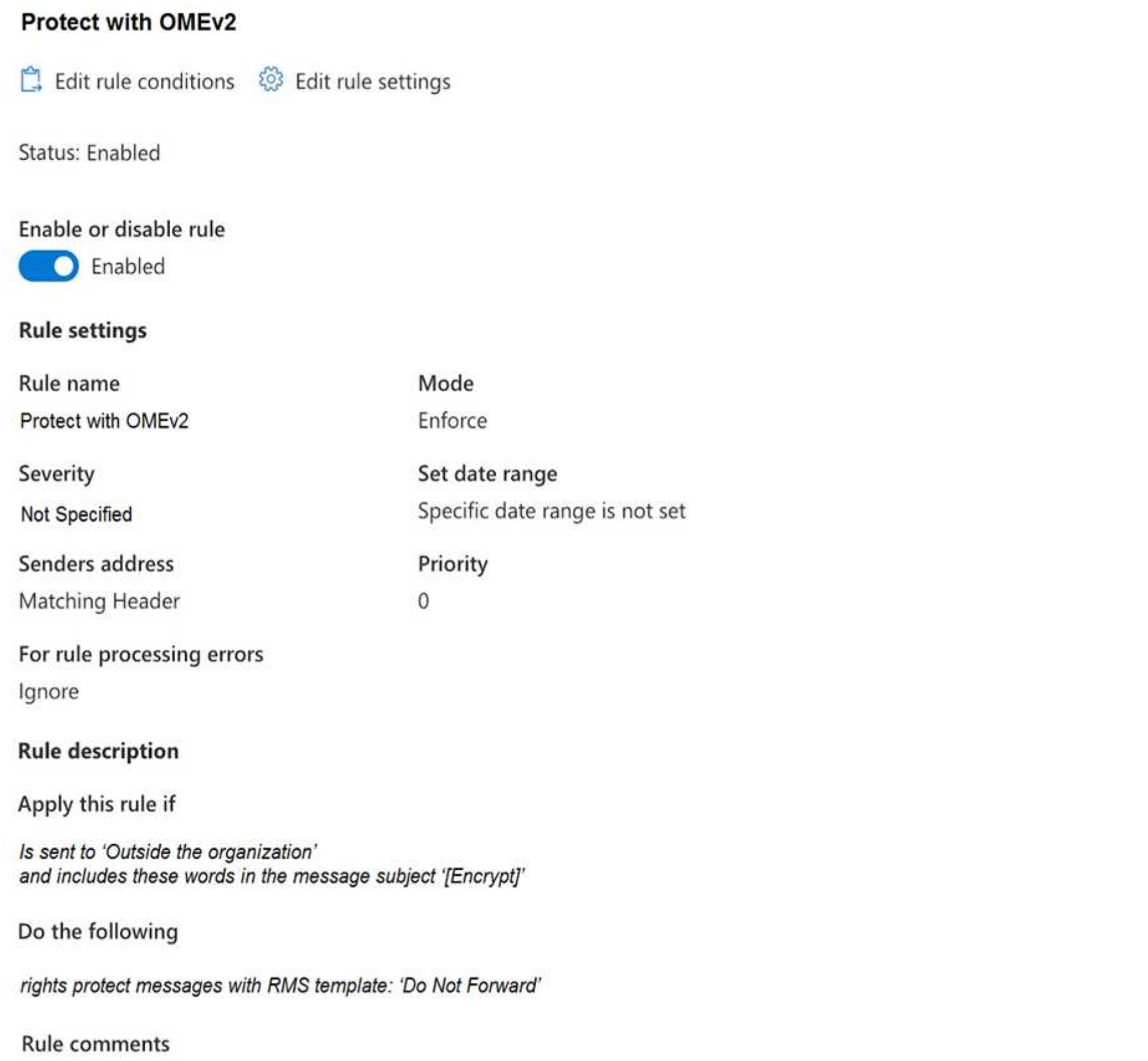
EXAM SC-401 TOPIC 1 QUESTION 66 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 66
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

You have a Microsoft 365 E5 subscription.

In Microsoft Exchange Online, you have the mail flow rule shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

Answer Area

Recipients who use Gmail
- must sign in to the Office 365 Message Encryption (OME) portal to read messages
- will be unable to read messages
- will have messages decrypted automatically

Recipients from an external Microsoft 365 subscription
- must sign in to the Office 365 Message Encryption (OME) portal to read messages
- will be unable to read messages
- will have messages decrypted automatically

Hide Answer

Suggested Answer:

Answer Area

Recipients who use Gmail: must sign in to the Office 365 Message Encryption (OME) portal to read messages

Recipients from an external Microsoft 365 subscription: will have messages decrypted automatically

by Kamiles at *Aug. 25, 2025, 3:35 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Gmail: must use O365 Message Encryption (OME) portal to read
External M365 org: will have email decrypted automatically (under certain conditions)

upvoted 3 times

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 67 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 67

Topic #: 1

[All SC-401 Questions]

You have a Microsoft 365 subscription.

You create a new trainable classifier.

You need to train the classifier.

Which source can you use to train the classifier?

A. an on-premises Microsoft SharePoint Server site

B. an Azure Files share

C. a Microsoft SharePoint Online site Most Voted

D. an NFS file share

Hide Answer

Suggested Answer: *C*

Community vote distribution

C (100%)

by JohnyBest at *Sept. 2, 2025, 8:16 p.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: C

C is correct answer: Online Sharepoint site

upvoted 3 times

florinvele 2 months, 4 weeks ago

Selected Answer: C

SharePoint Online folder

upvoted 1 times

JohnyBest 3 months, 1 week ago

Selected Answer: C

In Microsoft 365 Compliance, trainable classifiers are trained using content stored in Microsoft 365 services, because the classifier needs to access the data through cloud APIs.
Supported sources include:
SharePoint Online sites
OneDrive for Business
Exchange Online mailboxes
Not supported for training:
On-premises SharePoint
Azure Files
NFS shares

upvoted 4 times

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 68 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 68

Topic #: 1

[All SC-401 Questions]

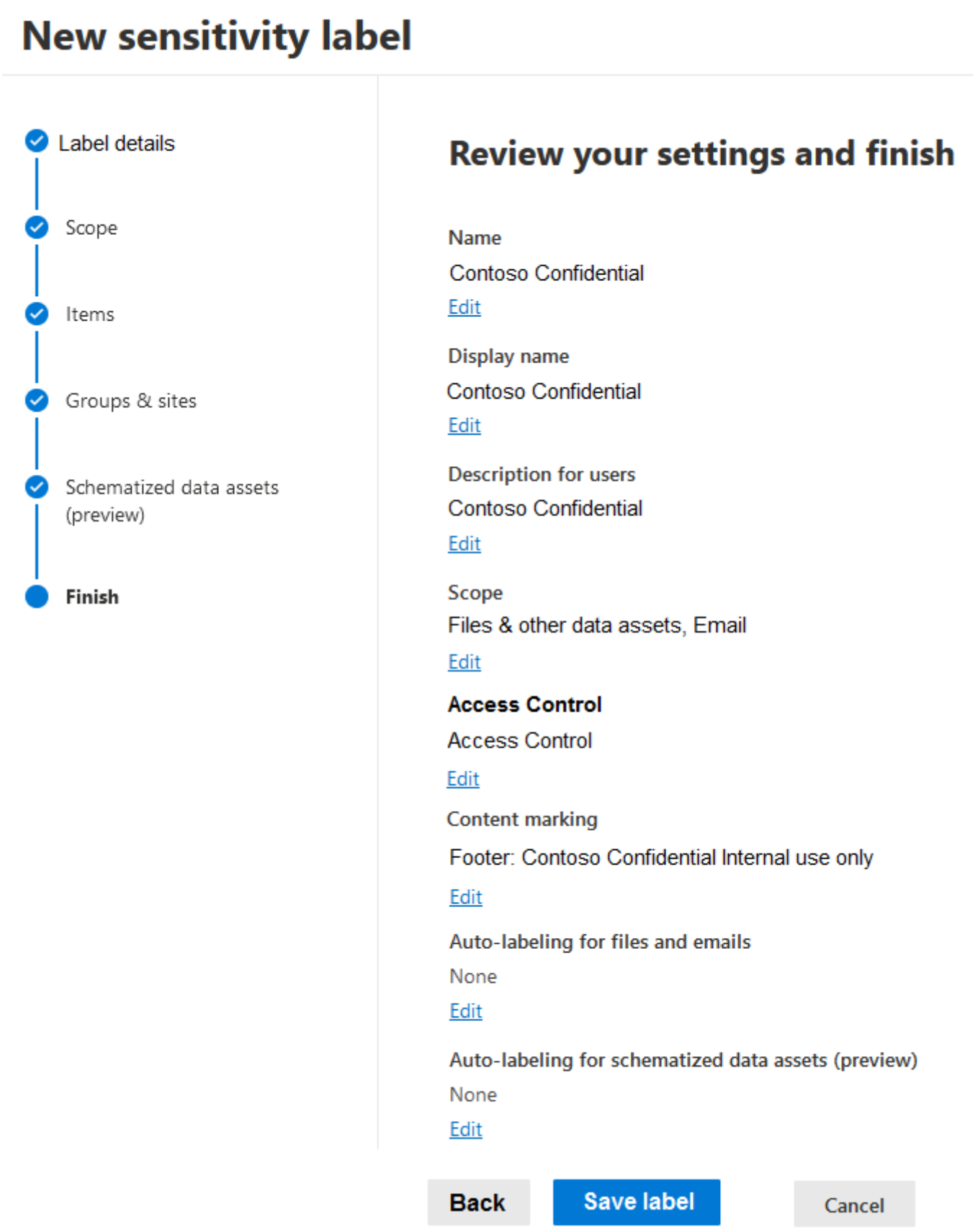
HOTSPOT

-

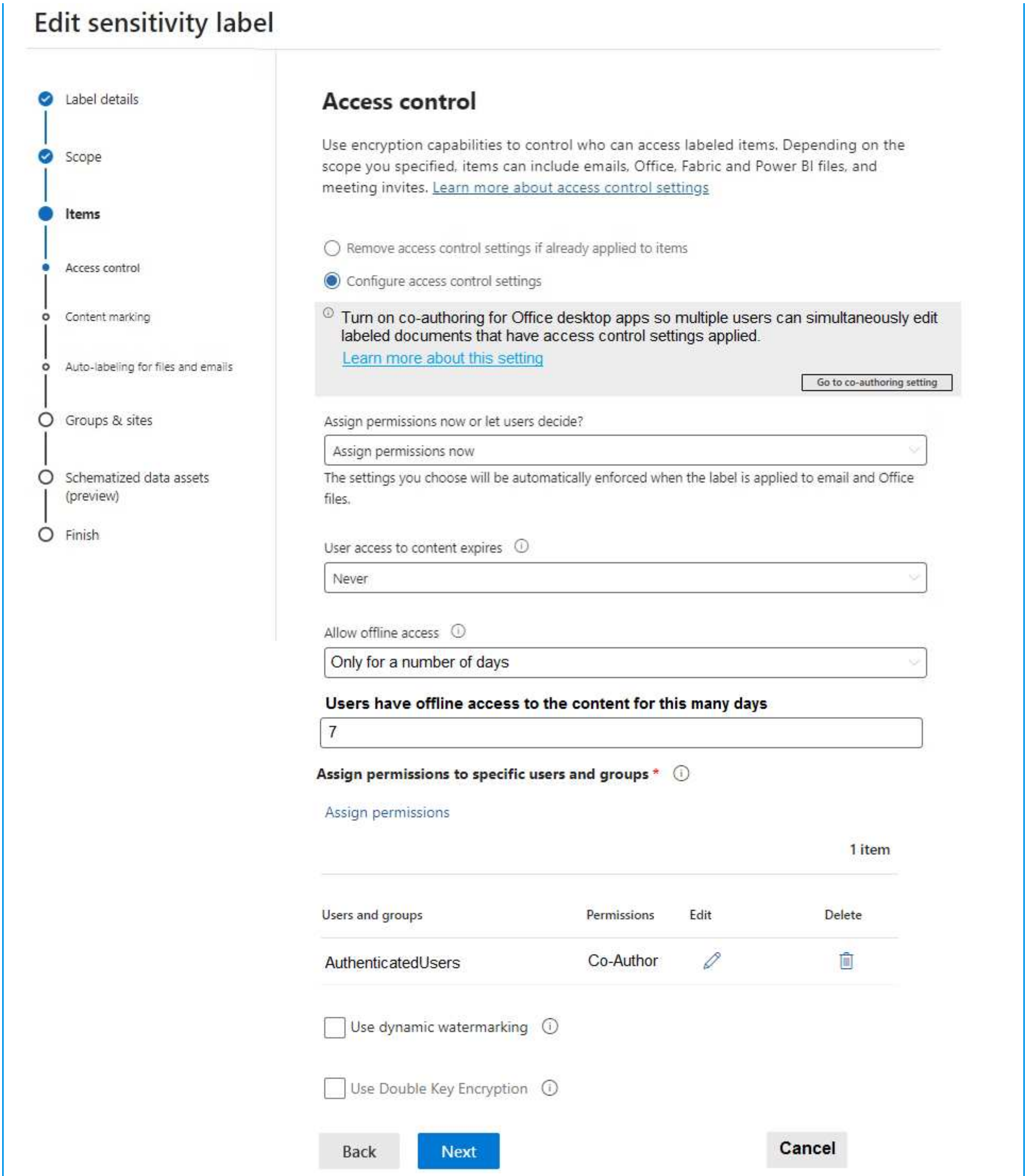
You have a Microsoft 365 subscription that contains a sensitivity label named Contoso Confidential.

You publish Contoso Confidential to all users.

Contoso Confidential is configured as shown in the Configuration exhibit. (Click the Configuration tab.)



The Access control settings of Contoso Confidential are configured as shown in the Access control exhibit. (Click the Access control tab.)


Edit sensitivity label
Label details
Scope
Items
Access control
Content marking
Auto-labeling for files and emails
Groups & sites
Schematized data assets (preview)
Finish
Access control
Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. Learn more about access control settings
Remove access control settings if already applied to items
Configure access control settings
Turn on co-authoring for Office desktop apps so multiple users can simultaneously edit labeled documents that have access control settings applied.
Learn more about this setting
Go to co-authoring setting
Assign permissions now or let users decide?
Assign permissions now
The settings you choose will be automatically enforced when the label is applied to email and Office files.
User access to content expires
Never
Allow offline access
Only for a number of days
Users have offline access to the content for this many days
7
Assign permissions to specific users and groups *
Assign permissions
1 item
Users and groups
Permissions
Edit
Delete
AuthenticatedUsers
Co-Author
Use dynamic watermarking
Use Double Key Encryption
Back
Next
Cancel

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If a user account is disabled, the user will be immediately prevented from opening a file protected by Contoso Confidential.	○	○
Guest users will be able to open documents protected by Contoso Confidential.	○	○
Contoso Confidential will be applied automatically to the files stored in Microsoft SharePoint. Online.	○	○

Hide Answer

Suggested Answer:

Answer Area

Statements	Yes	No
If a user account is disabled, the user will be immediately prevented from opening a file protected by Contoso Confidential.	○	☐
Guest users will be able to open documents protected by Contoso Confidential.	○	☐
Contoso Confidential will be applied automatically to the files stored in Microsoft SharePoint. Online.	○	☐

by Seidor_Analytics at *Sept. 5, 2025, 8:14 a.m.*

Comments

skalolaz Highly Voted 3 months, 1 week ago

I would say NYN, guest users are authenticated users.

upvoted 7 times

Ender3 Highly Voted 2 months ago

Yes, disabled accounts have no access to any content, and even offline the file is protected by the sensitivity label.

Yes, Guest users are authenticated users.

No, no auto-labeling policy was set.

upvoted 6 times

Eltooth Most Recent 2 months, 2 weeks ago

Yes - only Authenticated Users are allowed
Yes - Guests are authenticated on Contoso through Entra or federated social provider or authenticated by a Microsoft account.
No - SharePoint is not listed in scope (Groups & sites)

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 69 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 69
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

You have a Microsoft 365 E5 subscription.

You have a Microsoft Purview Advanced Message Encryption branding template named OME1.

You need to create a Microsoft Exchange Online mail flow rule to apply OME1 to email.

How should you configure the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Apply this rule if:

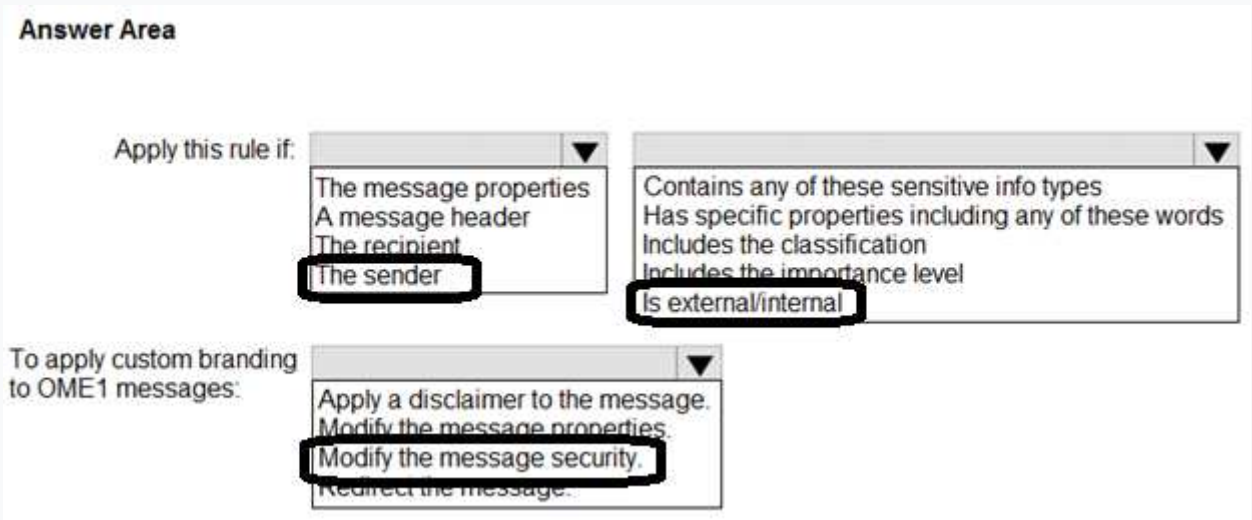
The message properties A message header The recipient The sender	Contains any of these sensitive info types Has specific properties including any of these words Includes the classification Includes the importance level Is external/internal

To apply custom branding to OME1 messages:

Apply a disclaimer to the message. Modify the message properties. Modify the message security. Redirect the message.

Hide Answer

Suggested Answer:


Answer Area
Apply this rule if:
The message properties
A message header
The recipient
The sender
Contains any of these sensitive info types
Has specific properties including any of these words
Includes the classification
Includes the importance level
Is external/internal
To apply custom branding to OME1 messages:
Apply a disclaimer to the message.
Modify the message properties.
Modify the message security.

by Seidor_Analytics at *Sept. 5, 2025, 8:14 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Looks like the question is missing some key info.

upvoted 4 times

florinvele 2 months, 4 weeks ago

First box: The RECIPIENT is internal/external

upvoted 1 times

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 70 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 70

Topic #: 1

[All SC-401 Questions]

You have a sensitive information type based on a trainable classifier.

You are unsatisfied with the result of the trainable classifier.

You need to retrain the classifier.

What should you use in the Microsoft Purview portal?

A. Content explorer from Data classification Most Voted

B. Labels from information protection

C. Labels from information governance

D. Content search

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:14 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: A

A is correct answer: Content Explorer

upvoted 1 times

msuan 2 months, 3 weeks ago

Selected Answer: A

A is correct

upvoted 3 times

florinvele 2 months, 4 weeks ago

Selected Answer: A

Content Explorer

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 71 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 71

Topic #: 1

[All SC-401 Questions]

You have a Microsoft 365 tenant that is opt-in for trainable classifiers.

You need to ensure that a user named User1 can create custom trainable classifiers. The solution must use the principle of least privilege.

Which role should you assign to User1?

A. Security Administrator

B. Compliance Administrator Most Voted

C. Global Administrator

D. Security Operator

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:14 a.m.*

Comments

RickySmith 2 months, 2 weeks ago

Selected Answer: B

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#compliance-administrator

upvoted 1 times

Eltooth 2 months, 2 weeks ago

Selected Answer: B

B is correct answer: Compliance Admin

upvoted 1 times

QuwQuw 2 months, 3 weeks ago

Selected Answer: B

Copilot: B

upvoted 4 times

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 72 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 72

Topic #: 1

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription.

You create a sensitivity label named Label1 and publish Label1 to all users and groups.

You have the following files in a SharePoint site:

- File1.doc
- File2.docx
- File3.xlsx
- File4.txt

You need to identify which files can have Label1 applied.

Which files should you identify?

A. File2.docx only

B. File2.docx and File3.xlsx only Most Voted

C. File1.doc, File2.docx, and File3.xlsx only

D. File1.doc, File2.doc, File3.xlsx, and File4.txt

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:15 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: B

B is correct answer: File22.doxc and File3.xlsx

Sensitivity labels in Microsoft Purview can be applied to files stored in SharePoint Online based on supported file types. The supported file types for automatic and manual labelling include:
.docx (Word)
.xlsx (Excel)
.pptx (PowerPoint)
These are modern Office file formats that support built-in labelling and encryption.
Unsupported files:
File1.doc: This is a legacy Word format and does not support sensitivity labels.
File4.txt: Plain text files are not supported for sensitivity labelling.

upvoted 1 times

QuwQuw 2 months, 3 weeks ago

Selected Answer: B

Copilot: B

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 73 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 73
Topic #: 1
[All SC-401 Questions]

You need to test Microsoft Purview Advanced Message Encryption capabilities for your company. The test must verify the following information:

• The acquired default template names
• The encryption and decryption verification status

Which PowerShell cmdlet should you run?

A. Test-OAuthConnectivity
B. Test-ClientAccessRule
C. Test-IRMConfiguration Most Voted
D. Test-Mailflow

Hide Answer

Suggested Answer: *C*

Community vote distribution
C (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:13 a.m.*

Comments

RickySmith 2 months, 2 weeks ago

Selected Answer: C

https://learn.microsoft.com/en-us/purview/set-up-new-message-encryption-capabilities#verify-microsoft-purview-message-encryption-configuration-in-exchange-online-powershell

upvoted 1 times

Eltooth 2 months, 2 weeks ago

Selected Answer: C

C is correct answer: Test-IRMConfiguration

upvoted 1 times

QuwQuw 2 months, 3 weeks ago

Selected Answer: C

Copilot: C

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 74 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 74

Topic #: 1

[All SC-401 Questions]

At the end of a project, you upload project documents to a Microsoft SharePoint Online library that contains many files. The following is a sample of the project document file names:

- aei_AA989.docx
- bci_WS098.docx
- cei_DF112.docx
- ebc_QQ454.docx
- ecc_BB565.docx

All documents that use this naming format must be labeled as Project Documents:

You need to create an auto-apply retention label policy.

What should you use to identify the files?

A. A retention label

B. A trainable classifier

C. A sensitive info type Most Voted

Hide Answer

Suggested Answer: *C*

Community vote distribution

C (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:15 a.m.*

Comments

florinvele Highly Voted 2 months, 4 weeks ago

Selected Answer: C

SIT with a regex as pattern

upvoted 5 times

Eltooth Most Recent 2 months, 2 weeks ago

Selected Answer: C

C is correct answer: Sensitive info type
https://learn.microsoft.com/en-us/purview/apply-retention-labels-automatically
You can configure auto-apply retention label policies based on:
Sensitive information types
Keywords or searchable properties
Trainable classifiers

In your scenario, where the filenames follow a structured format like:
aei_AA989.docx
bci_WS098.docx
cei_DF112.docx

“You can apply retention labels to content automatically when that content doesn't already have a retention label applied and contains sensitive information, keywords or searchable properties, or a match for trainable classifiers.”

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 75 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 75

Topic #: 1

[All SC-401 Questions]

DRAG DROP

-

You have a Microsoft 365 tenant.

A new regulatory requirement states that all documents containing a patent ID be labeled, retained for 10 years, and then deleted. The policy used to apply the retention settings must never be disabled or deleted by anyone.

You need to implement the regulatory requirement.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions		Answer Area
Add a management lock.		
Create a retention label.	1	
Create a retention policy.	2	
Create a retention label policy.	3	
Add a preservation lock.		

Hide Answer

Suggested Answer:

Answer Area	
1	Create a retention label.
2	Create a retention label policy.
3	Add a preservation lock.

by Seidor_Analytics at *Sept. 5, 2025, 8:14 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Create a retention label
Create a (Auto-Apply) retention label policy
Add a preservation lock (powershell) or Mark the item as a regulatory record

upvoted 2 times

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 76 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 76

Topic #: 1

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 tenant.

You need to create a new sensitive info type for items that contain the following:

• An employee ID number that consists of the hire date of the employee followed by a three digit number
• The words "Employee", "ID", or "Identification" within 300 characters of the employee ID number

What should you use for the primary and secondary elements? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Primary element:

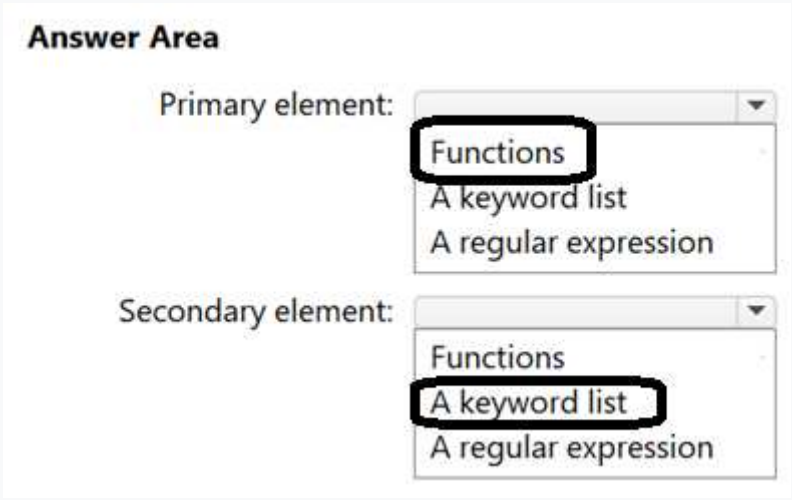
- Functions
- A keyword list
- A regular expression

Secondary element:

- Functions
- A keyword list
- A regular expression

Hide Answer

Suggested Answer:



by Leon1969 at *Oct. 29, 2025, 3:07 p.m.*

Comments

Pavol_Misun Highly Voted 1 month ago

I would vote for:
Primary element → A regular expression
Secondary element → A keyword list

upvoted 8 times

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 77 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 77

Topic #: 1

[All SC-401 Questions]

You plan to implement Microsoft Purview Advanced Message Encryption.

You need to ensure that encrypted email sent to external recipients expires after seven days.

What should you create first?

A. a mail flow rule

B. an X.509 version 3 certificate

C. a custom branding template

D. a remote domain in Microsoft Exchange

E. a connector in Microsoft Exchange

Hide Answer

Suggested Answer: *C*

Community vote distribution

C (100%)

by qvtszlfg9z at *Dec. 5, 2025, 9:29 p.m.*

Comments

AlejandroCaSa 2 days, 13 hours ago

Selected Answer: C

A custom branding template because that's where the message expiration and other options are defined.

upvoted 1 times

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 78 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 78

Topic #: 1

[All SC-401 Questions]

HOTSPOT

-

You are implementing Microsoft Purview Advanced Message Encryption for a Microsoft 365 tenant named contoso.com.

You need to meet the following requirements:

• All email to a domain named fabrikam.com must be encrypted automatically.
• Encrypted emails must expire seven days after they are sent.

What should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

All email to a domain named fabrikam.com must be encrypted automatically:

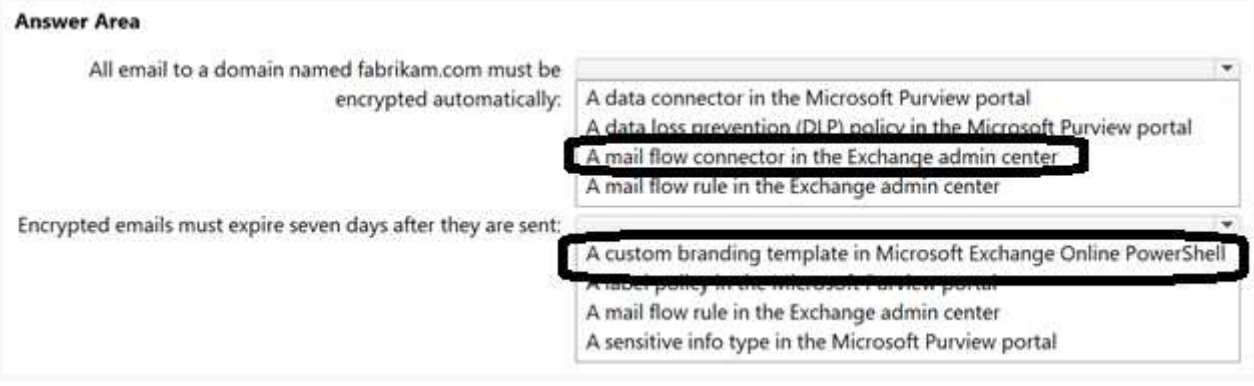
- A data connector in the Microsoft Purview portal
- A data loss prevention (DLP) policy in the Microsoft Purview portal
- A mail flow connector in the Exchange admin center
- A mail flow rule in the Exchange admin center

Encrypted emails must expire seven days after they are sent:

- A custom branding template in Microsoft Exchange Online PowerShell
- A label policy in the Microsoft Purview portal
- A mail flow rule in the Exchange admin center
- A sensitive info type in the Microsoft Purview portal

Hide Answer

Suggested Answer:


Answer Area
All email to a domain named fabrikam.com must be encrypted automatically:
A data connector in the Microsoft Purview portal
A mail flow connector in the Exchange admin center
A mail flow rule in the Exchange admin center
Encrypted emails must expire seven days after they are sent:
A custom branding template in Microsoft Exchange Online PowerShell
A mail flow rule in the Exchange admin center
A sensitive info type in the Microsoft Purview portal

by Leon1969 at *Oct. 29, 2025, 3:11 p.m.*

Comments

Alcpt Highly Voted 1 month, 1 week ago

With Microsoft Purview Advanced Message Encryption, anytime you apply custom branding, Microsoft 365 applies the wrapper to email that fits the mail flow rule to which you apply the template. You can only use expiration if you use custom branding.
#1 mail flow rule
#2 custom branding

upvoted 6 times

EXAMTOPICS

Microsoft Discussions

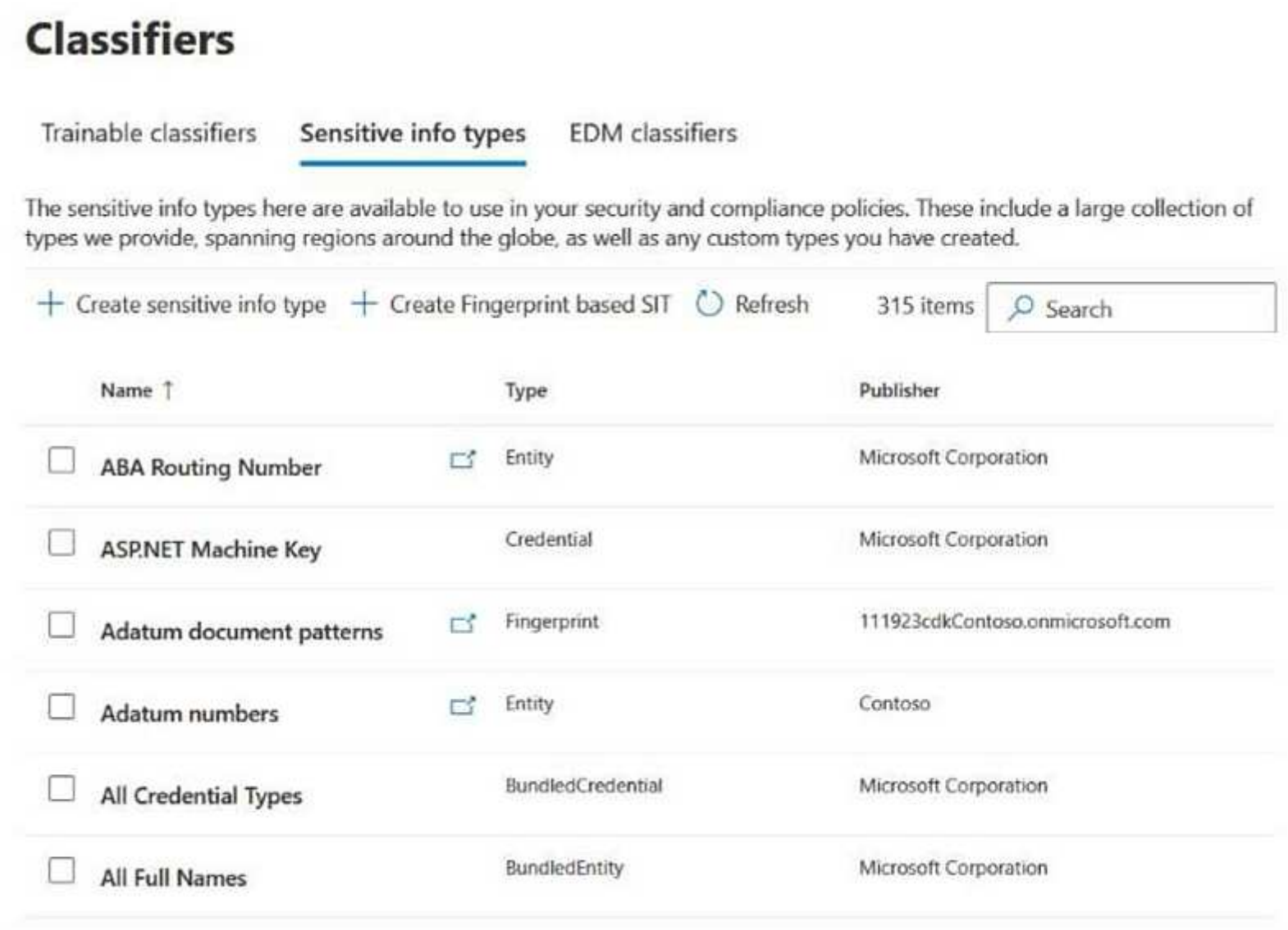
Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 80 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 80
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

You have a Microsoft 365 subscription that contains the sensitive information types (SITs) shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

To create a new SIT, you can copy **[answer choice]**.

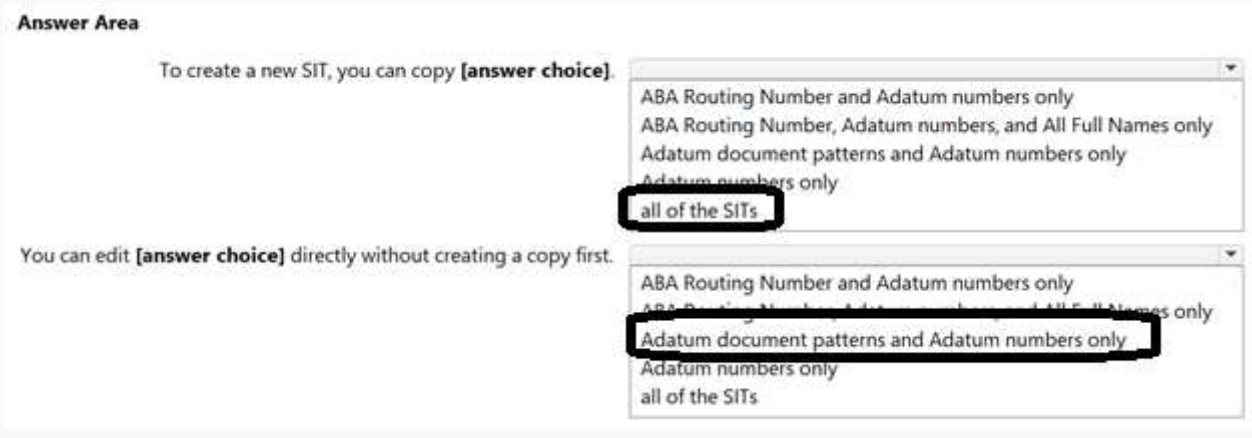
- ABA Routing Number and Adatum numbers only
- ABA Routing Number, Adatum numbers, and All Full Names only
- Adatum document patterns and Adatum numbers only
- Adatum numbers only
- all of the SITs

You can edit **[answer choice]** directly without creating a copy first.

- ABA Routing Number and Adatum numbers only
- ABA Routing Number, Adatum numbers, and All Full Names only
- Adatum document patterns and Adatum numbers only
- Adatum numbers only
- all of the SITs

Hide Answer

Suggested Answer:


Answer Area
To create a new SIT, you can copy [answer choice].
ABA Routing Number and Adatum numbers only
ABA Routing Number, Adatum numbers, and All Full Names only
Adatum document patterns and Adatum numbers only
all of the SITs
You can edit [answer choice] directly without creating a copy first.
ABA Routing Number and Adatum numbers only
Adatum document patterns and Adatum numbers only
Adatum numbers only
all of the SITs

by Alcpt at *Nov. 5, 2025, 2:52 p.m.*

Comments

bobg 2 weeks, 2 days ago

Can copy ABA Routing Number and Adatum Numbers only
Can edit Adatum Numbers Only

upvoted 1 times

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 81 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 81

Topic #: 1

[All SC-401 Questions]

You have a Microsoft 365 subscription that contains 100 users and a Microsoft 365 group named Group1.

All users have Windows 11 devices and use Microsoft SharePoint Online and Exchange Online.

A sensitivity label named Label1 is published as the default label for Group1.

You add two sublabels named Sublabel1 and Sublabel2 to Label1.

You need to ensure that the settings in Sublabel1 are applied by default to Group1.

What should you do?

A. Modify the policy of Label1.

B. Duplicate all the settings from Sublabel1 to Label1.

C. Delete the policy of Label1 and publish Sublabel1.

D. Change the order of Sublabel1.

Hide Answer

Suggested Answer: *C*

Community vote distribution

D (75%) C (25%)

by Alcpt at *Nov. 5, 2025, 3:01 p.m.*

Comments

Blabla532 3 days, 21 hours ago

Selected Answer: C

Cannot set a sublabel as the default directly. The default label must be the parent label that is published in the policy.

upvoted 1 times

Alcpt 1 month, 1 week ago

Selected Answer: D

✅ Correct Answer:
D. Change the order of Sublabel1.
❌ Why not the others?
A. Modify the policy of Label1 → This changes parent label settings, not which sublabel is default.
B. Duplicate settings from Sublabel1 to Label1 → Still applies Label1 by default, not Sublabel1.
C. Delete Label1 and publish Sublabel1 → Breaks hierarchy and is unnecessary.

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 82 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 82

Topic #: 1

[All SC-401 Questions]

You have a Microsoft 365 E5 tenant that contains a user named User1. User1 is assigned the Compliance Administrator role.

User1 cannot view the regular expression in the IP Address sensitive info type.

You need to ensure that User1 can view the regular expression.

What should you do?

A. Assign User1 the Global Reader role.

B. Assign User1 to the Reviewer role group.

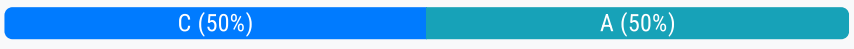
C. Create a copy of the IP Address sensitive info type and instruct User1 to edit the copy.

D. Instruct User1 to use the Test function on the sensitive info type.

Hide Answer

Suggested Answer: *C*

Community vote distribution



by bobg at *Nov. 24, 2025, 4:36 p.m.*

Comments

AlejandroCaSa 2 days, 12 hours ago

Selected Answer: C

You can't view or edit the primary pattern (such as regex) for built-in sensitive information types. To customize, you must create a copy

upvoted 1 times

mlstud 4 days, 23 hours ago

Selected Answer: A

Global Reader

upvoted 1 times

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 84 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 84
Topic #: 1
[All SC-401 Questions]

You have a Microsoft 365 E5 subscription.

You have a Microsoft SharePoint Online document library that contains Microsoft Word and Excel documents. The documents contain the following types of information:

- Credit card numbers
- Physical addresses in the UK
- National health service numbers from the UK
- Sensitive projects that contain the following words: Project Tailspin, Project Contoso, and Project Falcon

You have email messages in Microsoft Exchange Online that contain the following information types:

- Credit card numbers
- User sign-in credentials
- National health service numbers from the UK

You plan to use sensitive information types (SITs) for compliance policies.

What is the minimum number of SITs required to classify all the information types?

A. 2

B. 5 Most Voted

C. 7

D. 10

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (100%)

by Alcpt at *Nov. 5, 2025, 3:21 p.m.*

Comments

Pavol_Misun 1 month ago

Selected Answer: B

5.

SharePoint Online documents contain:

Credit card numbers → Use the built-in SIT: Credit Card Number.
Physical addresses in the UK → Use the built-in SIT: UK Address.
National Health Service numbers (UK) → Use the built-in SIT: UK NHS Number.
Sensitive project names → Requires a custom SIT (or a trainable classifier) for keywords like Project Tailspin, Project Contoso, Project Falcon.

Exchange Online emails contain:

User sign-in credentials → Use the built-in SIT: Credentials (or Authentication Information).

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 85 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 85
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Email address	Distribution group
User1	user1@contoso.com	Finance
User2	user2@contoso.com	Sales

You create the data loss prevention (DLP) policies shown in the following table.

Name	Order	Apply policy to	Conditions	Actions	Exceptions	User notifications	Additional options
Policy1	0	Exchange email for the Finance distribution group	Content shared with people outside my organization. Content contains five or more credit card numbers.	Encrypt the message by using the Encrypt email messages option.	user4@fabrikam.com	Send an incident report to the administrator.	If there's a match for this rule, stop processing additional DLP policies and rules.
Policy2	1	All locations of Exchange email	Content shared with people outside my organization. Content contains five or more credit card numbers.	Restrict access or encrypt the content in Microsoft 365 locations. Block only people outside your organization.	*None*	Send an incident report to the administrator.	*None*

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If User1 sends an email message that contains five credit card numbers to user4@fabrikam.com, the message will be encrypted.	○	○
If User1 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered.	○	○
If User2 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered.	○	○

Hide Answer

Suggested Answer:

Answer Area

Statements	Yes	No
If User1 sends an email message that contains five credit card numbers to user4@fabrikam.com, the message will be encrypted.	○	◉
If User1 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered.	◉	○
If User2 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered.	○	◉

by evrybobry at *Nov. 3, 2025, 6:23 p.m.*

Comments

mlstud 4 days, 23 hours ago

Given answers are correct.

upvoted 1 times

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 86 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 86

Topic #: 1

[All SC-401 Questions]

You have a Microsoft 365 E5 tenant that has a retention label named Label1.

You need to create an auto-labeling policy that will apply Label1.

To which location can Label1 be applied?

A. OneDrive accounts

B. Microsoft Entra security groups

C. Microsoft Defender for Cloud Apps

D. Teams chats

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (100%)

by t5qkye4nqb at *Dec. 5, 2025, 8:51 p.m.*

Comments

AlejandroCaSa 2 days, 11 hours ago

Selected Answer: A

given answer is correct. Currently, Teams chats and Microsoft Defender for cloud apps do not support auto-labeling, only retention policies.

upvoted 1 times

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 87 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 87

Topic #: 1

[All SC-401 Questions]

You receive an email that contains a list of words that will be used for a sensitive information type.

You need to create a file that can be used as the source of a keyword dictionary.

In which format should you save the list?

A. a JSON file that has an element for each word

B. a DOCX file that has one word on each line

C. a CSV file that contains words separated by commas

D. an ACCDB database file that contains a table named Dictionary

Hide Answer

Suggested Answer: *C*

Community vote distribution

C (100%)

by j435c9yytb at *Dec. 5, 2025, 8:51 p.m.*

Comments

AlejandroCaSa 2 days, 11 hours ago

Selected Answer: C

On the Add a keyword dictionary flyout, you can:

Upload a dictionary file in TXT or CSV format.
Choose from existing dictionaries.
or create a new dictionary by entering keywords manually and giving it a name.

https://learn.microsoft.com/en-us/purview/sit-create-a-keyword-dictionary

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 92 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 92
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

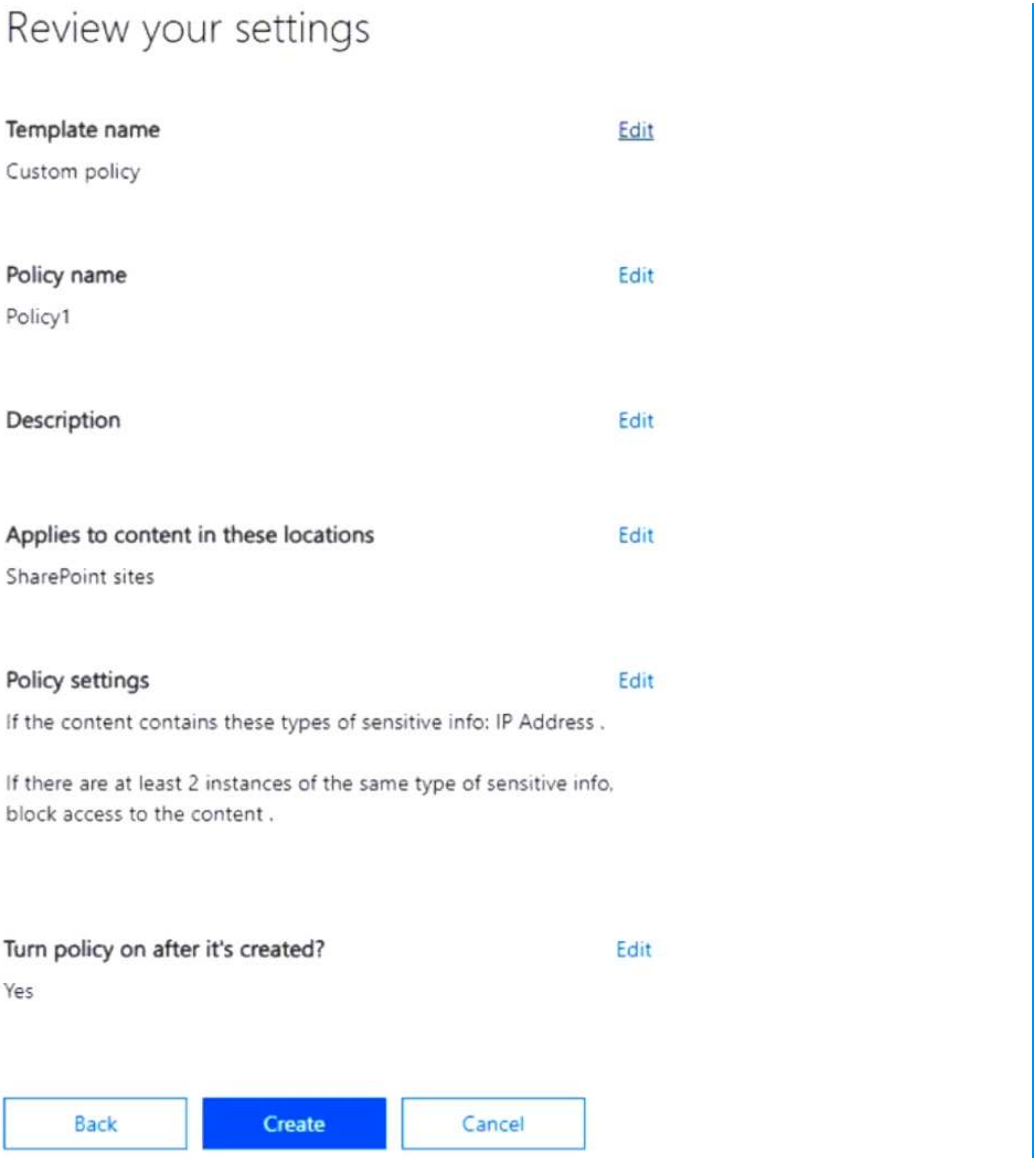
You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

You have a Microsoft SharePoint site named Site1. Site1 stores files that contain IP addresses as shown in the following table.

Name	Number of IP addresses
File1.txt	3
File2.docx	1

User1 is assigned the SharePoint admin role for Site1. User2 is a member of Site1.

You create the data loss prevention (DLP) policy shown in the following exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can view the contents of File1.txt.	○	○
User2 can view the contents of File1.txt.	○	○
User2 can view the contents of File2.docx.	○	○

Hide Answer

Suggested Answer:

by bobg at *Nov. 25, 2025, 9:28 a.m.*

Comments

bobg 2 weeks, 4 days ago

NNY for me. Admins cant open a file thats blocked by DLP either.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam
Go to Exam

EXAM SC-401 TOPIC 1 QUESTION 94 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 94
Topic #: 1
[All SC-401 Questions]

HOTSPOT
-

You have a Microsoft 365 tenant named contoso.com that contains two users named User1 and User2. The tenant uses Microsoft Purview Message Encryption.

User1 plans to send emails that contain attachments as shown in the following table.

Subject	To	Attachment type	Message size
Mail1	User2@contoso.com	.docx	40 MB
Mail2	User4@outlook.com	.doc	3 MB
Mail3	User3@gmail.com	.xlsx	7 MB

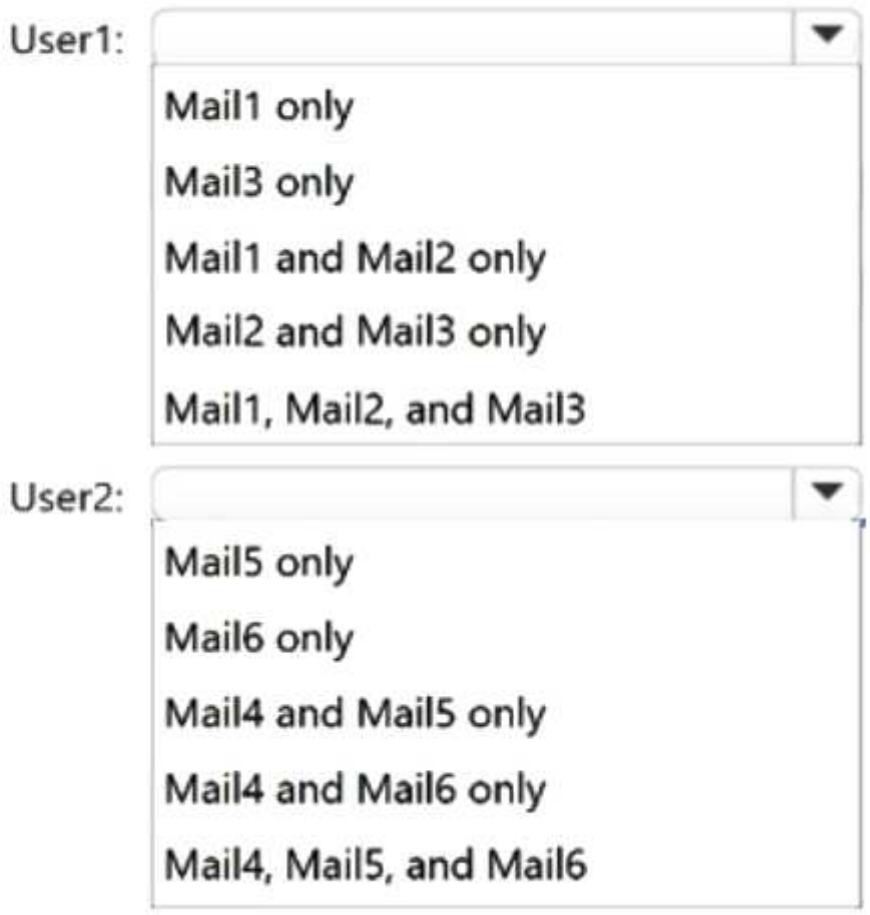
User2 plans to send emails that contain attachments as shown in the following table.

Subject	To	Attachment type	Message size
Mail4	User1@contoso.com	.pptx	4 MB
Mail5	User4@outlook.com	.jpg	6 MB
Mail6	User3@gmail.com	.docx	3 MB

For which emails will the attachments be encrypted? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Hide Answer

Suggested Answer:

by ADUSAM at *Nov. 19, 2025, 11:30 p.m.*

Comments

bobg 2 weeks, 4 days ago

Agree with the answer here

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 2 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 2

Topic #: 2

[All SC-401 Questions]

HOTSPOT -

Case Study -

Instructions -

This is a case study. Case studies are not timed separately from other exam sections. You can use as much exam time as you would like to complete each case study. However, there might be additional case studies or other exam sections. Manage your time to ensure that you can complete all the exam sections in the time provided. Pay attention to the Exam Progress at the top of the screen so you have sufficient time to complete any exam sections that follow this case study.

To answer the case study questions, you will need to reference information that is provided in the case. Case studies and associated questions might contain exhibits or other resources that provide more information about the scenario described in the case. Information provided in an individual question does not apply to the other questions in the case study.

A Review Screen will appear at the end of this case study. From the Review Screen, you can review and change your answers before you move to the next exam section. After you leave this case study, you will NOT be able to return to it.

To start the case study -

To display the first question in this case study, select the "Next" button. To the left of the question, a menu provides links to information such as business requirements, the existing environment, and problem statements. Please read through all this information before answering any questions. When you are ready to answer a question, select the "Question" button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.

Existing Environment -

Microsoft 365 Environment -

Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

Users store data in the following locations:

SharePoint sites -

OneDrive accounts -

Exchange email -

Exchange public folders -

Teams chats -

Teams channel messages -

Teams channel messages -
When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

SharePoint Online Environment -
Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.
Site2 contains the files shown in the following table.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.
Site4 has the following two retention policies applied:

Name: Site4RetentionPolicy1 -
Locations to apply the policy: Site4
Delete items older than: 2 years
Delete content based on: When items were created

Name: Site4RetentionPolicy2 -
Locations to apply the policy: Site4
Retain items for a specific period: 4 years
Start the retention period based on: When items were created
At the end of the retention period: Do nothing

Problem Statements -
Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

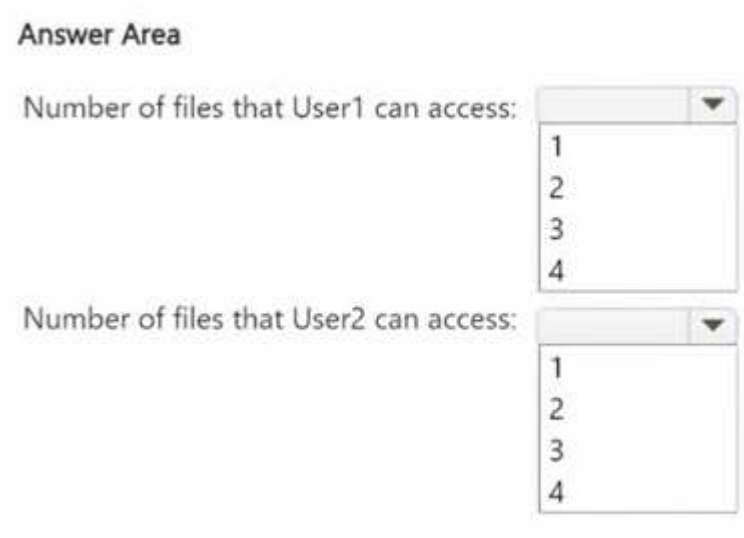
Requirements -

Planned Changes -
Contoso plans to create the following data loss prevention (DLP) policy:

Name: DLPpolicy1 -
Locations to apply the policy: Site2
Conditions:
Content contains any of these sensitive info types: SWIFT Code

Instance count: 2 to any -
Actions: Restrict access to the content

Technical Requirements -
Contoso must meet the following technical requirements:
All administrative users must be able to review DLP reports.
Whenever possible, the principle of least privilege must be used.
For all users, all Microsoft 365 data must be retained for at least one year.
Confidential documents must be detected and protected by using Microsoft 365.
Site1 documents that include credit card numbers must be labeled automatically.
All administrative users must be able to create Microsoft 365 sensitivity labels.
After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.
How many files in Site2 can User1 and User2 access after you turn on DLPpolicy1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Hide Answer

Suggested Answer:

by leprechaun at *May 27, 2025, 7:33 a.m.*

Comments

Linpus Highly Voted 6 months, 2 weeks ago
User1 as site owner: all 4 files
User2: 2 files (File1.docx and File2.bmp)
upvoted 11 times

papillor 6 months, 1 week ago
Agreed !
upvoted 1 times

zied01 5 months ago
User 2 only one file : file2.bmp , docx is blocked by the dlp

upvoted 1 times

zied01 4 months, 3 weeks ago

sorry i didn't so the number occurence , so user 2 : 2 files

upvoted 1 times

PsiCzar 6 months, 2 weeks ago

There is no mention of OCR being enabled, so it shouldnt detect the swift code in the bmp image file.

upvoted 4 times

deeptha92 Highly Voted 3 months, 2 weeks ago

User 1 (Site Owner) - 4 Files
User 2 (Site Visitor) 2 Files

Any item that makes it through the conditions filter has any actions that are defined in the rule applied to it. You have to configure the required options to support the action. For example, if you select Exchange with the Restrict access or encrypt the content in Microsoft 365 locations action, you need to choose from these options:

Block users from accessing shared SharePoint, OneDrive, and Teams content
Block everyone. Only the content owner, last modifier, and site admin will continue to have access
Block only people from outside your organization. Users inside your organization continue to have access.
Encrypt email messages (applies only to content in Exchange)
The actions that are available in a rule depend on the locations that have been selected. The available actions for each individual location are listed below.

upvoted 6 times

Alcpt Most Recent 1 month, 1 week ago

I think its
4
1
The Technical Requirements says:
Confidential documents must be detected and protected by using Microsoft 365, which means that the Microsoft Purview DLP solution supports scanning .bmp files for sensitive information when the OCR setting is enabled at the tenant level and configured in the policy. Once enabled, the policy can detect sensitive data (like credit card numbers or social security numbers) within the image and enforce protective actions.

upvoted 1 times

Ender3 2 months ago

User1: 4 files
User2: 2 files

This is a tricky question with incomplete information. The SIT used to identify files containing SWIFT codes will work on Office documents and txt files, but it will not work on images unless OCR is enabled. There is no mention of OCR.

Assuming no OCR, and given that File1.docx has only 1 SWIFT code, the DLP policy will restrict access to only File3.txt and File4.xlsx.

Moving on, when creating a policy rule in Purview to restrict access, it explicitly states this: "For files in SharePoint, OneDrive, and teams, only the owner, last modifier, and site admin will have access."

"owner" here refers to the owner of the file, but site owner is also a site admin, therefore User1 is not restricted from accessing any files. Only User2 is restricted from accessing the two files mentioned.

upvoted 2 times

Eltooth 2 months, 2 weeks ago

User 1 (Site Owner) - 4 Files
User 2 (Site Visitor) 2 Files

upvoted 1 times

RickySmith 3 months ago

4,2
https://learn.microsoft.com/en-us/purview/dlp-policy-reference#actions

upvoted 3 times

DrArjunReddy 4 months, 2 weeks ago

4 and 2

upvoted 4 times

4d76265 6 months ago

Does anyone have evidence of where "site owner" can bypass DLP actions?

I think the answer is:
User1:2 files
User2:2 files

I don't think site owner can bypass DLP actions and no mention of OCR being enabled (disabled by default) so I would have to go for 2 files for both. Happy to be corrected if I am wrong.

upvoted 3 times

bobg 2 weeks, 4 days ago

I agree with this. No-one can bypass DLP as far as i know unless override is enabled. An admin can change the rule or disable the rule.

upvoted 1 times

leprechaun 6 months, 2 weeks ago

User1 (Site Owner): Site Owners typically bypass DLP restrictions, so User1 can access all files.

User2 (Site Visitor): Site Visitors are restricted by DLP policies, so User2 can access only file1.docx.

upvoted 5 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 4 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 4

Topic #: 2

[All SC-401 Questions]

Case Study -

Instructions -

This is a case study. Case studies are not timed separately from other exam sections. You can use as much exam time as you would like to complete each case study. However, there might be additional case studies or other exam sections. Manage your time to ensure that you can complete all the exam sections in the time provided. Pay attention to the Exam Progress at the top of the screen so you have sufficient time to complete any exam sections that follow this case study.

To answer the case study questions, you will need to reference information that is provided in the case. Case studies and associated questions might contain exhibits or other resources that provide more information about the scenario described in the case. Information provided in an individual question does not apply to the other questions in the case study.

A Review Screen will appear at the end of this case study. From the Review Screen, you can review and change your answers before you move to the next exam section. After you leave this case study, you will NOT be able to return to it.

To start the case study -

To display the first question in this case study, select the "Next" button. To the left of the question, a menu provides links to information such as business requirements, the existing environment, and problem statements. Please read through all this information before answering any questions. When you are ready to answer a question, select the "Question" button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.

Existing Environment -

Microsoft 365 Environment -

Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

Users store data in the following locations:

SharePoint sites -

OneDrive accounts -

Exchange email -

Exchange public folders -

Teams chats -

Teams channel messages -
When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

SharePoint Online Environment -
Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.
Site2 contains the files shown in the following table.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.
Site4 has the following two retention policies applied:

Name: Site4RetentionPolicy1 -
Locations to apply the policy: Site4
Delete items older than: 2 years
Delete content based on: When items were created

Name: Site4RetentionPolicy2 -
Locations to apply the policy: Site4
Retain items for a specific period: 4 years
Start the retention period based on: When items were created
At the end of the retention period: Do nothing

Problem Statements -
Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

Requirements -

Planned Changes -
Contoso plans to create the following data loss prevention (DLP) policy:

Name: DLPpolicy1 -
Locations to apply the policy: Site2
Conditions:
Content contains any of these sensitive info types: SWIFT Code

Instance count: 2 to any -
Actions: Restrict access to the content

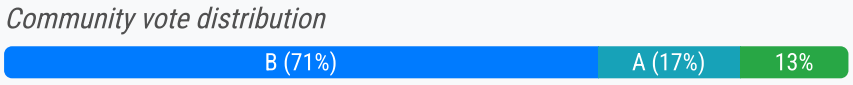
Technical Requirements -
Contoso must meet the following technical requirements:
All administrative users must be able to review DLP reports.
Whenever possible, the principle of least privilege must be used.
For all users, all Microsoft 365 data must be retained for at least one year.
Confidential documents must be detected and protected by using Microsoft 365.
Site1 documents that include credit card numbers must be labeled automatically.
All administrative users must be able to create Microsoft 365 sensitivity labels.
After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.
You need to meet the retention requirement for the users' Microsoft 365 data.
What is the minimum number of retention policies required to achieve the goal?

A. 1
B. 2 **Most Voted**
C. 3
D. 4
E. 6

Hide Answer

Suggested Answer: *B*

Community vote distribution



by Linpus at *May 27, 2025, 1:39 p.m.*

Comments

papillor Highly Voted 6 months, 1 week ago

Selected Answer: B

1 - One policy to retrain all MS 365 data for at least one year. (globally)
2 - One policy to retain the documents for 10 years on Site3.

upvoted 6 times

PsiCzar Highly Voted 6 months, 2 weeks ago

Selected Answer: B

The answer is correct.

"If you select the Teams or Viva Engage locations when you create a retention policy, the other locations are automatically excluded. " So you would need 2 policies to select all of the location in the case study. https://learn.microsoft.com/en-us/purview/create-retention-policies?tabs=teams-retention

upvoted 5 times

nuin01 Most Recent 3 weeks, 6 days ago

Selected Answer: C

Policy1 : SharePoint sites, OneDrive accounts, Exchange email, Exchange public folders
Policy2: Teams chats and Teams channel messages
Policy3: Retain documents that relate to completed projects for 10 years on Site3

upvoted 1 times

Eltooth 2 months, 2 weeks ago

Selected Answer: B

B is correct answer: 2 policies
One for SPO, ODfB, Exchange/public
One for Teams

Note: If question asks for Co--pilot, Enterprise AI or Other AI apps - these are also individual and cannot be shared with others.

upvoted 1 times

deeptha92 3 months, 2 weeks ago

Selected Answer: B

Agree with most here. Its 2 policies.
1 for SharePoint sites, Exchange Mailboxes, and Public Folders,
2nd policy for Teams Chats and Channel messages

The requirement to preserve some data in Site 3 for 10 years is achieved by retention labels

upvoted 3 times

ppolychron 4 months, 1 week ago

Selected Answer: C

You cannot select Teams workloads with other 365 services for retention policies.

Policy1 : SharePoint sites, OneDrive accounts, Exchange email, Exchange public folders
Policy2: Teams chats and Teams channel messages
Policy3: Retain documents that relate to completed projects for 10 years on Site3

upvoted 2 times

tila_s 4 months, 3 weeks ago

Selected Answer: A

Project data should be retained via retention label. Only 1 retention policy is required

upvoted 1 times

4d76265 6 months ago

Selected Answer: B

Look at where the 365 user data is stored in environment section - SharePoint sites, OneDrive accounts, Exchange email, Exchange public folders, Teams chats and Teams channel messages.

You cannot mix Teams workloads with other 365 services for retention policies - the Purview GUI won't allow this so therefore 2 policies must be created.

upvoted 2 times

KrisDeb 6 months, 2 weeks ago

Selected Answer: A

You need only one retention policy scoped to Site3, with a 10-year retention duration.

upvoted 2 times

Linpus 6 months, 2 weeks ago

Selected Answer: A

You can create a single Microsoft Purview retention policy that targets all Microsoft 365 locations (Exchange mailboxes, SharePoint sites, OneDrive accounts, Teams channel messages, and Teams chats) and set the retention period to one year. That one policy will cover every user’s data across Microsoft 365 for the required minimum one-year retention.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 5 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 5

Topic #: 2

[All SC-401 Questions]

HOTSPOT -

You have a Microsoft SharePoint Online site that contains the following files.

Name	Modified by	Data loss prevention (DLP) action
File1.docx	Manager1	*None*
File2.docx	Manager1	Matched by DLP
File3.docx	Manager1	Blocked by DLP

Users are assigned roles for the site as shown in the following table.

Name	Role
User1	Site owner
User2	Site member

Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

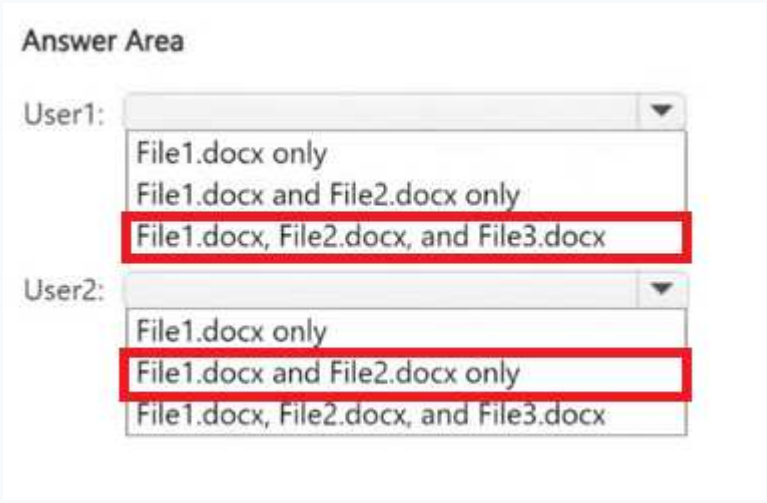
Answer Area

User1:
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

User2:
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

Hide Answer

Suggested Answer:



by CuentaRM10 at *June 3, 2025, 5:57 p.m.*

Comments

gabbinu Highly Voted 3 months, 3 weeks ago

User1 (site owner): File1.docx, File2.docx, and File3.docx
User2 (site member): File1.docx and File2.docx only

Reason: When a DLP policy blocks a SharePoint file, access is restricted to the site owner, the document owner, and the last modifier. "Matched by DLP" (without a block action) doesn't restrict access. Here, File3.docx is Blocked by DLP, so the site owner (User1) can open it, but a regular member (User2) cannot. All users can open File1 and File2.

upvoted 9 times

RickySmith 3 months ago

https://learn.microsoft.com/en-us/purview/dlp-policy-reference#actions

upvoted 1 times

4d76265 Highly Voted 6 months ago

Does anyone have evidence of where "site owner" can bypass DLP actions?

Matched by DLP means audited/logged but not block.

User1: Files 1 and 2
User2: Files 1 and 2

upvoted 8 times

nuin01 3 weeks, 6 days ago

I tested it in an environment, and if the user is not the creator of the file or the last person to modify it, a site owner doesn't see it, unlike an administrator who does.

upvoted 1 times

zied01 5 months, 1 week ago

the site owner is the site admin , dlp will block access for all users except the doc owner and the site admin/owner

upvoted 4 times

Koenst 6 months ago

I Agree, and so does chatGPT and Copilot

upvoted 2 times

Eltooth Most Recent 2 months, 2 weeks ago

User1 (site owner): File1.docx, File2.docx, and File3.docx
User2 (site member): File1.docx and File2.docx only

upvoted 1 times

RickySmith 3 months ago

3,2
https://learn.microsoft.com/en-us/purview/dlp-policy-reference#actions

upvoted 2 times

landfils 5 months, 1 week ago

Correct. https://learn.microsoft.com/en-us/purview/dlp-policy-reference

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 6 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 6
Topic #: 2
[All SC-401 Questions]

You are planning a data loss prevention (DLP) solution that will apply to Windows Client computers.
You need to ensure that when users attempt to copy a file that contains sensitive information to a USB storage device, the following requirements are met:
If the users are members of a group named Group1, the users must be allowed to copy the file, and an event must be recorded in the audit log.
All other users must be blocked from copying the file.
What should you create?

A. one DLP policy that contains one DLP rule

B. one DLP policy that contains two DLP rules

C. two DLP policies that each contains one DLP rule **Most Voted**

Hide Answer

Suggested Answer: *C*

Community vote distribution

C (95%) 5%

by DiegoWill at *April 21, 2025, 8:40 p.m.*

Comments

DiegoWill **Highly Voted** 7 months, 3 weeks ago

Selected Answer: C

It is not possible within the same device policy to select a group or user under the conditions of the rule, so you need 2 policies and each with a rule.

upvoted 8 times

KrisDeb **Highly Voted** 6 months, 2 weeks ago

Selected Answer: C

In Microsoft Purview DLP, when configuring device-based DLP policies (specifically for Windows endpoint DLP), user or group targeting is done at the policy level, not at the rule level. This means:
• You cannot target different user groups within a single policy rule for device control actions (like USB copy).
• Therefore, to apply different behaviours based on group membership, you must create separate policies targeting each group.

upvoted 6 times

Eltooth Most Recent 2 months, 2 weeks ago

Selected Answer: C

C is correct answer: 2 DLP policies that each contain one DLP rule

upvoted 1 times

gabbinu 3 months, 3 weeks ago

Selected Answer: C

In Microsoft Purview DLP, user or group targeting is done at the policy level, not at the rule level. This means you cannot target different user groups within a single policy, you must create separate policies targeting each group.

upvoted 2 times

454252dfr 4 months, 2 weeks ago

Selected Answer: B

One DLP policy keeps the configuration centralized and easier to manage.
Two DLP rules allow you to define different actions based on group membership:
Rule 1: Applies to Group1 → Allow + Audit.
Rule 2: Applies to everyone else → Block.

upvoted 1 times

CuentaRM10 6 months, 2 weeks ago

Selected Answer: C

Since you need a rule to audit the group you will need to create one policy for this specific task and another one that excludes the group and block the rest. Answer C is correct

upvoted 3 times

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 3 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 3
Topic #: 2
[All SC-401 Questions]

HOTSPOT -

Case Study -

Instructions -
This is a case study. Case studies are not timed separately from other exam sections. You can use as much exam time as you would like to complete each case study. However, there might be additional case studies or other exam sections. Manage your time to ensure that you can complete all the exam sections in the time provided. Pay attention to the Exam Progress at the top of the screen so you have sufficient time to complete any exam sections that follow this case study.
To answer the case study questions, you will need to reference information that is provided in the case. Case studies and associated questions might contain exhibits or other resources that provide more information about the scenario described in the case. Information provided in an individual question does not apply to the other questions in the case study.
A Review Screen will appear at the end of this case study. From the Review Screen, you can review and change your answers before you move to the next exam section. After you leave this case study, you will NOT be able to return to it.

To start the case study -
To display the first question in this case study, select the "Next" button. To the left of the question, a menu provides links to information such as business requirements, the existing environment, and problem statements. Please read through all this information before answering any questions. When you are ready to answer a question, select the "Question" button to return to the question.

Overview -
Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.

Existing Environment -

Microsoft 365 Environment -
Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

Users store data in the following locations:

SharePoint sites -

OneDrive accounts -

Exchange email -

Exchange public folders -

Teams chats -

Teams channel messages -

Teams channel messages -
When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

SharePoint Online Environment -
Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.
Site2 contains the files shown in the following table.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.
Site4 has the following two retention policies applied:

Name: Site4RetentionPolicy1 -
Locations to apply the policy: Site4
Delete items older than: 2 years
Delete content based on: When items were created

Name: Site4RetentionPolicy2 -
Locations to apply the policy: Site4
Retain items for a specific period: 4 years
Start the retention period based on: When items were created
At the end of the retention period: Do nothing

Problem Statements -
Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

Requirements -

Planned Changes -
Contoso plans to create the following data loss prevention (DLP) policy:

Name: DLPpolicy1 -
Locations to apply the policy: Site2
Conditions:
Content contains any of these sensitive info types: SWIFT Code

Instance count: 2 to any -
Actions: Restrict access to the content

Technical Requirements -
Contoso must meet the following technical requirements:
All administrative users must be able to review DLP reports.
Whenever possible, the principle of least privilege must be used.
For all users, all Microsoft 365 data must be retained for at least one year.
Confidential documents must be detected and protected by using Microsoft 365.
Site1 documents that include credit card numbers must be labeled automatically.
All administrative users must be able to create Microsoft 365 sensitivity labels.
After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.
You are reviewing policies for the SharePoint Online environment.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If a user creates a file in Site4 on January 1, 2021, users will be able to access the file on January 15, 2023.	○	○
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2023.	○	○
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2026.	○	○

Hide Answer

Suggested Answer:

Answer Area

Statements	Yes	No
If a user creates a file in Site4 on January 1, 2021, users will be able to access the file on January 15, 2023.	●	○
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2023.	●	○
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2026.	○	●

by PsiCzar at *June 12, 2025, 1:19 a.m.*

Comments

4d76265 Highly Voted 6 months ago
Given answers are correct. Retention policies take priority over deletion policies.
upvoted 5 times

Eltooth Most Recent 2 months, 2 weeks ago
Yes - 4 year retention policy wins over 2 year
Yes - file will still be retained - but hidden from perm deletion
No - time difference is >4 years to retention policy would perm delete
upvoted 2 times

PsiCzar 6 months ago

Correct.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 7 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 7

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 subscription.

You need to ensure that users can apply retention labels to individual documents in their Microsoft SharePoint libraries.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From Microsoft Defender for Cloud Apps, create a file policy.

B. From the SharePoint admin center, modify the Site Settings.

C. From the SharePoint ad min center, modify the records management settings.

D. From the Microsoft Purview portal, publish a label. **Most Voted**

E. From the Microsoft Purview portal, create a label. **Most Voted**

Hide Answer

Suggested Answer: *DE*

Community vote distribution

DE (100%)

by CuentaRM10 at *May 27, 2025, 2:28 p.m.*

Comments

CuentaRM10 **Highly Voted** 6 months, 2 weeks ago

Selected Answer: DE

The answer is correct

upvoted 6 times

Eltooth **Most Recent** 2 months, 2 weeks ago

Selected Answer: DE

D and E are correct.

upvoted 2 times

KrisDeb 6 months, 2 weeks ago

Selected Answer: DE

E. From the Microsoft Purview portal, create a label.
You must first create a retention label in Microsoft Purview (formerly Microsoft 365 Compliance Centre) that defines what happens to content (e.g. retain for 7 years, delete after 5 years, etc.).
D. From the Microsoft Purview portal, publish a label.
After creating the label, you must publish it to make it available for users to manually apply it to content in SharePoint (and OneDrive, Outlook, etc.).

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 8 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 8

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.

You need to implement Microsoft Purview data lifecycle management.

What should you create first?

A. a sensitivity label policy

B. a data loss prevention (DLP) policy

C. an auto-labeling policy

D. a retention label **Most Voted**

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (100%)

by KrisDeb at *May 28, 2025, 9:07 p.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: D

D is correct answer: Retention label

upvoted 2 times

KrisDeb 6 months, 2 weeks ago

Selected Answer: D

To implement Microsoft Purview Data Lifecycle Management (formerly part of Microsoft Information Governance), the first step is typically to create a retention label.

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 9 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 9

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription.

You need to create static retention policies for the following locations:

Teams chats -

Exchange email -

SharePoint sites -

Microsoft 365 Groups -

Teams channel messages -

What is the minimum number of retention policies required?

A. 1

B. 2 **Most Voted**

C. 3

D. 4

E. 5

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (57%) C (39%) 4%

by DiegoWill at *April 21, 2025, 9:02 p.m.*

Comments

DiegoWill **Highly Voted** 7 months, 3 weeks ago

Selected Answer: B

Only 2 policies are needed because it is not possible to contain team chats and channels together with the other workloads (Exchange, SPO and M365 groups).

upvoted 10 times

papillor 6 months, 1 week ago

I'd tend to agree with 2 policies too, but if you go on Purview, on the retention policy creation section, there's no more "Teams chats" nor "Teams channel messages".

upvoted 2 times

Blabla532 Most Recent 4 days, 14 hours ago

Selected Answer: C

3 required, u cannot create a single Purview retention policy that covers all Teams chats (1:1, group chats) and all channel messages (standard, private, shared) simultaneously; you need separate policies for different Teams locations like "Teams chats" (private/group) and "Teams channel messages,"

upvoted 1 times

Eltooth 2 months, 2 weeks ago

Selected Answer: B

B is correct answer: 2 retention policies.

upvoted 1 times

Eltooth 2 months, 2 weeks ago

NOTE: If you see Teams Private channel messages - they are also stand alone.

In Purview you now will see this message:
"Messages from Teams private channels. (NOTE: Will be deprecated by Oct 2025. Please use Teams channel messages policy for Private channels.) "

upvoted 2 times

Gtc_ 3 months, 2 weeks ago

Selected Answer: C

3 policies. Teams Chat, Teams Channel, All others

upvoted 1 times

ivzdf 4 months, 2 weeks ago

Selected Answer: B

Although a retention policy can support multiple services that are identified as "locations" in the retention policy, you can't create a single retention policy that includes all the supported locations:

Exchange mailboxes
SharePoint sites or SharePoint classic and communication sites
OneDrive accounts
Microsoft 365 Group mailboxes & sites
Skype for Business
Exchange public folders
Teams channel messages
Teams chats
Teams private channel messages
Microsoft Copilot experiences
Enterprise AI apps
Other AI apps
Viva Engage community messages
Viva Engage user messages
If you select the Teams or Viva Engage locations when you create a retention policy, the other locations are automatically excluded. This means that the instructions to follow depend on whether you need to include the Teams or Viva Engage locations.https://learn.microsoft.com/en-us/purview/create-retention-policies?view=o365-worldwide&tabs=teams-retention

upvoted 2 times

tila_s 4 months, 3 weeks ago

Selected Answer: C

Policy 1 – for Teams chats

Policy 2 – for Teams channel messages

Policy 3 – combined for:

Exchange mailboxes

SharePoint sites

Microsoft 365 Groups

upvoted 4 times

10319ae 5 months ago

Selected Answer: C

Correct me if I'm wrong, but this is the answer from Copilot

It's a clever thought—but no, you can't reduce it to just two retention policies if you want to cover all five locations with static scopes.
📌 Why You Need Three
- Teams chats and Teams channel messages are treated as separate workloads in Microsoft Purview. Each requires its own retention policy.
- Exchange email, SharePoint sites, and Microsoft 365 Groups can be bundled into a single policy.
So even with the most efficient configuration, you still need:
- One policy for Teams chats
- One policy for Teams channel messages
- One policy for Exchange, SharePoint, and Microsoft 365 Groups

upvoted 3 times

7259dc7 5 months, 4 weeks ago

Selected Answer: A

You can now have a single retention policy for Sharepoint, Onedrive, Exchange, 365 groups and Teams stuff

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 10 DISCUSSION

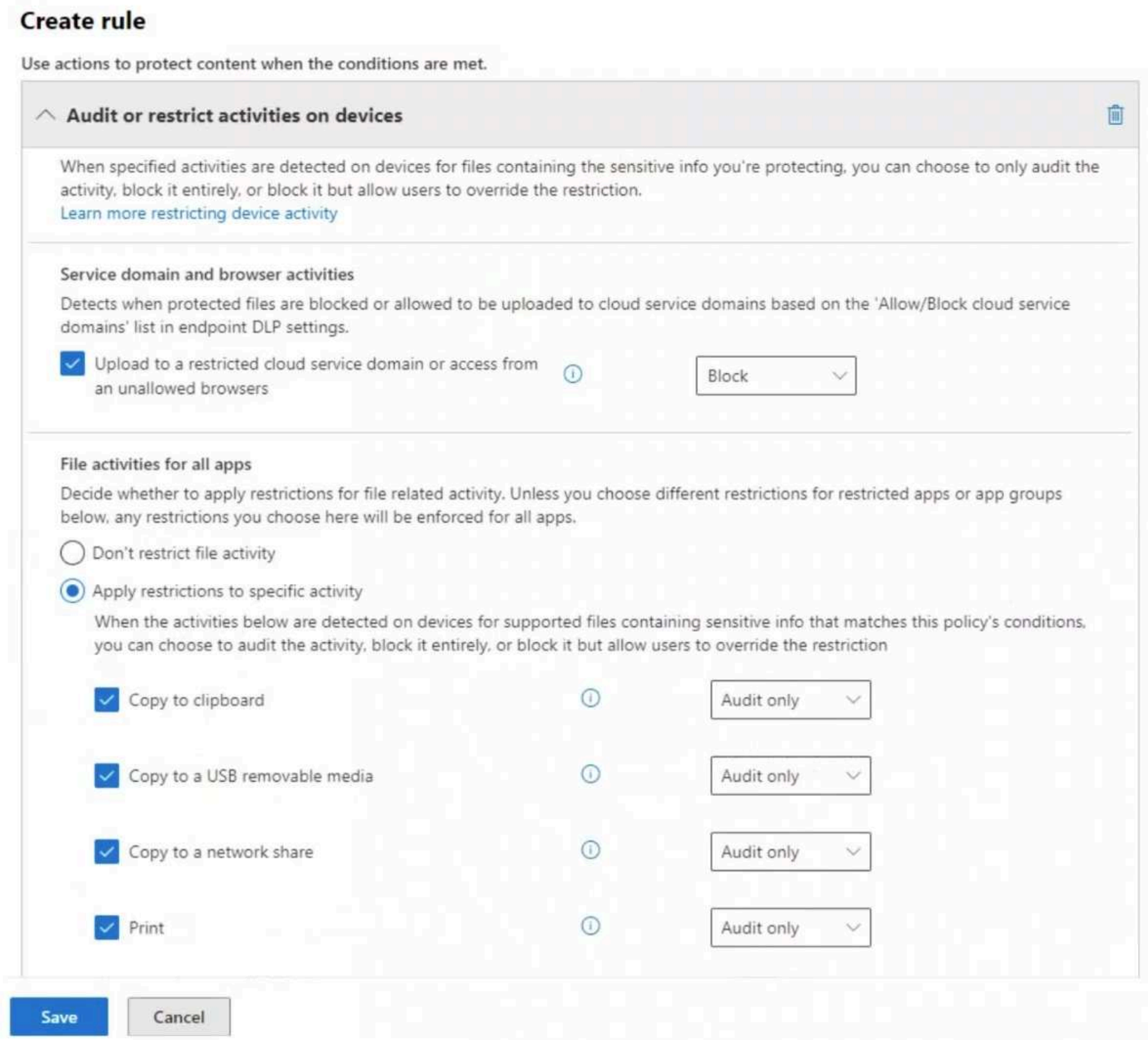
Actual exam question from Microsoft's SC-401

Question #: 10

Topic #: 2

[All SC-401 Questions]

You have a data loss prevention (DLP) policy configured for endpoints as shown in the following exhibit.


Create rule
Use actions to protect content when the conditions are met.
Audit or restrict activities on devices
When specified activities are detected on devices for files containing the sensitive info you're protecting, you can choose to only audit the activity, block it entirely, or block it but allow users to override the restriction.
Learn more restricting device activity
Service domain and browser activities
Detects when protected files are blocked or allowed to be uploaded to cloud service domains based on the 'Allow/Block cloud service domains' list in endpoint DLP settings.
Upload to a restricted cloud service domain or access from an unallowed browsers
Block
File activities for all apps
Decide whether to apply restrictions for file related activity. Unless you choose different restrictions for restricted apps or app groups below, any restrictions you choose here will be enforced for all apps.
Don't restrict file activity
Apply restrictions to specific activity
When the activities below are detected on devices for supported files containing sensitive info that matches this policy's conditions, you can choose to audit the activity, block it entirely, or block it but allow users to override the restriction
Copy to clipboard
Audit only
Copy to a USB removable media
Audit only
Copy to a network share
Audit only
Print
Audit only
Save
Cancel

From a computer named Computer1, a user can sometimes upload files to cloud services and sometimes cannot. Other users experience the same issue.

What are two possible causes of the issue? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. The unallowed browsers in the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings are NOT configured. **Most Voted**

B. There are file path exclusions in the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings. **Most Voted**

C. The Access by restricted apps action is set to Audit only.

D. The Copy to clipboard action is set to Audit only.

E. The computers are NOT onboarded to Microsoft Purview.

Hide Answer

Suggested Answer: *AB*

Community vote distribution

AB (84%) AE (16%)

by KrisDeb at *May 28, 2025, 9:26 p.m.*

Comments

gabbinu Highly Voted 3 months, 3 weeks ago

Selected Answer: AB

A. If the unallowed browser list is empty or misconfigured, behavior may be inconsistent across different browsers.

B.If exclusions are set for certain folders/paths, sometimes files bypass the restriction and sometimes they don't → explains "sometimes can, sometimes cannot."

It's not E because if devices weren't onboarded, DLP wouldn't apply at all. But here, restrictions are happening, so onboarding is fine.

upvoted 5 times

Katadaaa Highly Voted 6 months, 1 week ago

Selected Answer: AB

agree with A and B

don't forget "sometimes"

upvoted 5 times

Eltooth Most Recent 2 months, 2 weeks ago

Selected Answer: AB

A and B are correct. As per other answers.

upvoted 1 times

7259dc7 5 months, 3 weeks ago

Selected Answer: AB

The DLP policy is not applied to a computer that is not onboarded, so if a computer is not onboarded, it does not get any DLP restrictions

upvoted 3 times

7259dc7 5 months, 3 weeks ago

Selected Answer: AB

The DLP policy will is apply to a computer that is not onboarded

upvoted 2 times

KrisDeb 6 months, 2 weeks ago

Selected Answer: AE

A. The unallowed browsers in the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings are NOT configured.
If unallowed browsers are not configured, users might still be able to upload files via unsupported or unmonitored browsers. This can lead to inconsistent enforcement of DLP policies, depending on which browser is used.

E. The computers are NOT onboarded to Microsoft Purview.
For Endpoint DLP to apply and enforce rules, the devices must be onboarded to Microsoft Purview. If they are not, policies will not apply consistently, leading to the described issue.

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 11 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 11

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that contains a retention policy named RP1 as shown in the following table.

Setting	Value
Location	• Exchange email (All recipients) • SharePoint sites (All sites)
Retain items for a specific period	5 years (When items were created)
At the end of the retention period	Delete items automatically

You place a preservation lock on RP1.

You need to modify RP1.

Which two modifications can you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Add locations to the policy. **Most Voted**

B. Delete the policy.

C. Remove locations from the policy.

D. Decrease the retention period of the policy.

E. Disable the policy.

F. Increase the retention period of the policy. **Most Voted**

Hide Answer

Suggested Answer: *AF*

Community vote distribution

AF (100%)

by KrisDeb at *May 28, 2025, 9:29 p.m.*

Comments

Katadaaa Highly Voted 6 months, 1 week ago

Selected Answer: AF

When a retention policy is locked:
- No one can disable the policy or delete it
- Locations can be added but not removed
- You can extend the retention period but not decrease it

upvoted 8 times

KrisDeb Highly Voted 6 months, 2 weeks ago

Selected Answer: AF

A. Add locations to the policy
Correct – You can add locations to a locked retention policy because this action increases the scope of retention, which is permitted.
B. Delete the policy
Incorrect – You cannot delete a retention policy that has a preservation lock applied. The lock is intended to make the policy immutable in terms of data protection.
C. Remove locations from the policy
Incorrect – Removing locations reduces the scope of retention, which is disallowed under a preservation lock.
D. Decrease the retention period of the policy
Incorrect – You cannot decrease the retention period as it would reduce the time items are kept, violating the intent of the preservation lock.
E. Disable the policy
Incorrect – Disabling the policy would stop enforcement, which is also not permitted once a preservation lock is in place.
F. Increase the retention period of the policy
Correct – You can increase the retention period because this retains data for longer, which is allowed under a preservation lock.

upvoted 5 times

Eltooth Most Recent 2 months, 2 weeks ago

Selected Answer: AF

A and F are correct answers.

upvoted 1 times

deeptha92 3 months, 2 weeks ago

Selected Answer: AF

When a retention policy is locked:

No one can disable the policy or delete it
Locations can be added but not removed
You can extend the retention period but not decrease it

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 12 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 12

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 E5 tenant that has devices onboarded to Microsoft Defender for Endpoint as shown in the following table.

Name	Type
Device1	Windows 11
Device2	Windows 10
Device3	iOS
Device4	macOS

You plan to start using Microsoft 365 Endpoint data loss protection (Endpoint DLP).

Which devices support Endpoint DLP?

A. Device1 only

B. Device1 and Device2 only

C. Device1 and Device4 only

D. Device1, Device2, and Device4 only **Most Voted**

E. Device1, Device2, Device3, and Device4

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (100%)

by ETUs3r at *April 6, 2025, 6 a.m.*

Comments

CuentaRM10 **Highly Voted** 6 months, 2 weeks ago

Selected Answer: D

The correct answer should be D
https://learn.microsoft.com/en-us/purview/endpoint-dlp-learn-about

upvoted 7 times

Eltooth **Most Recent** 2 months, 2 weeks ago

Selected Answer: D

D is correct answer.

upvoted 2 times

landfils 5 months, 1 week ago

Selected Answer: D

Correct

upvoted 1 times

DiegoWill 7 months, 3 weeks ago

Selected Answer: D

The correct Answer should be D because MacOS must be onboarded.

https://learn.microsoft.com/en-us/purview/device-onboarding-macos-overview#before-you-begin

upvoted 2 times

ETUs3r 8 months, 1 week ago

Selected Answer: D

Correct Answer should be D.
https://learn.microsoft.com/en-us/purview/endpoint-dlp-learn-about

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 13 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 13

Topic #: 2

[All SC-401 Questions]

HOTSPOT -

You have a Microsoft 365 E5 subscription that contains two Microsoft 365 groups named Group1 and Group2. Both groups use the following resources:

A group mailbox -

Microsoft Teams channel messages

A Microsoft SharePoint Online teams site

You create the objects shown in the following table.

Name	Type	Description
RLabel1	Retention label	*None*
AutoApply1	Auto-labeling policy	Applies RLabel1 to Group1
Retention1	Retention policy	Applied to Group2

To which resources will AutoApply1 and Retention1 be applied? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

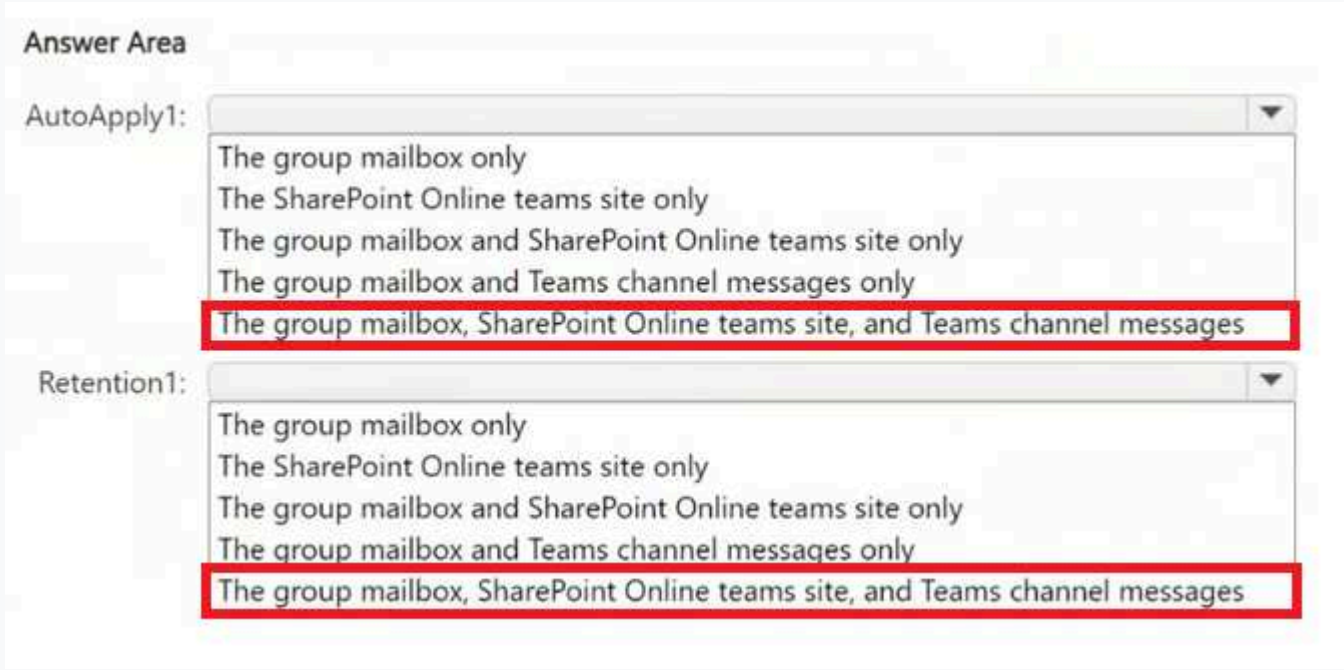
Answer Area

AutoApply1:
- The group mailbox only
- The SharePoint Online teams site only
- The group mailbox and SharePoint Online teams site only
- The group mailbox and Teams channel messages only
- The group mailbox, SharePoint Online teams site, and Teams channel messages

Retention1:
- The group mailbox only
- The SharePoint Online teams site only
- The group mailbox and SharePoint Online teams site only
- The group mailbox and Teams channel messages only
- The group mailbox, SharePoint Online teams site, and Teams channel messages

Hide Answer

Suggested Answer:


Answer Area
AutoApply1:
The group mailbox only
The SharePoint Online teams site only
The group mailbox and SharePoint Online teams site only
The group mailbox and Teams channel messages only
The group mailbox, SharePoint Online teams site, and Teams channel messages
Retention1:
The group mailbox only
The SharePoint Online teams site only
The group mailbox and SharePoint Online teams site only
The group mailbox and Teams channel messages only
The group mailbox, SharePoint Online teams site, and Teams channel messages

by DiegoWill at *April 21, 2025, 9:39 p.m.*

Comments

Eltooth 2 months ago

AutoApply1 → applies RLabel1 to Group1's mailbox and SharePoint site only, not Teams messages.
Retention1 → applies to Group2's mailbox, SharePoint site, and Teams channel messages.

upvoted 2 times

gabbinu 3 months, 3 weeks ago

AutoApply1: The group mailbox and SharePoint Online teams site only
Retention1: The group mailbox, SharePoint Online teams site, and Teams channel messages

Auto-labeling policies can only apply to Exchange mail (including group mailboxes) and SharePoint/OneDrive — not Teams messages.

Retention policies can apply to all three locations:
Group mailbox, SharePoint Online site and Teams channel messages

upvoted 2 times

Jdr379 5 months, 2 weeks ago

AutoApply1: The group mailbox and SharePoint Online teams site only
Retention1: The group mailbox, SharePoint Online teams site, and Teams channel messages

1. Auto-labeling policies for Microsoft 365 Groups apply to the group mailbox and SharePoint teams site, but not Teams channel messages directly
2. Retention policies for Microsoft 365 Groups have broader scope, covering the group mailbox, SharePoint teams site, and Teams channel messages
3. Teams chats or Teams channel messages that have their own retention policy locations are still included when the policy targets the Microsoft 365 Group directly

https://learn.microsoft.com/en-us/purview/retention-settings

upvoted 4 times

4d76265 6 months, 1 week ago

I think it should be:

AutoApply1: The group mailbox and SharePoint Online teams site only
Retention1: The group mailbox and SharePoint Online teams site only

Auto-labelling policy cannot be applied to Teams chat and channel messages. You cannot mix Teams workloads with other 365 services for retention policies so there must be 1 policy for Exchange and SharePoint and another policy for Teams.

upvoted 2 times

Katadaaa 6 months, 1 week ago

AutoApply1 : The group mailbox and SharePoint Online teams site only
Retention1 : The group mailbox and SharePoint Online teams site only
(need of two retention policies, one for mailbox/SPO and one for Teams)

upvoted 2 times

DiegoWill 7 months, 3 weeks ago

The answer should be:

The group mailbox and SharePoint Online teams site only
The group mailbox, SharePoint Online teams site, and Teams channel messages

Automatic retention label policies are not yet supported for Teams channel messages. It only applies to Exchange (mailbox) and SharePoint Online. Team channel messages only support files that are attached, not messages.

https://learn.microsoft.com/en-us/purview/apply-retention-labels-automatically#auto-apply-labels-to-cloud-attachments

upvoted 3 times

Newb007 7 months ago

I think it might be "The group mailbox and SharePoint Online teams site only" for both.

Why?
You cannot apply a group to the SharePoint Sites location in the Auto Label policy. you can only apply the group to the exchange location.

For the retention policy you cannot have one policy that covers both Team Channels Chats AND Group Mailbox/Team Sites. It won't let you toggle on both locations when creating. I just tested.

upvoted 1 times

Newb007 7 months ago

Sorry so the first one MIGHT be just the Group Mailbox. I'm torn on this one.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 14 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 14

Topic #: 2

[All SC-401 Questions]

HOTSPOT -

You have a Microsoft 365 E5 subscription that contains the device configurations shown in the following table.

Name	Type
Device1	Windows 11
Device2	Windows 10
Device3	iOS
Device4	macOS

Each configuration uses either Google Chrome or Firefox as a default browser.

You need to implement Microsoft Purview and deploy the Microsoft Purview browser extension to the configurations.

To which configuration can each extension be deployed? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Google Chrome:
- Config1 only
- Config2 only
- Config1 and Config2 only
- Config2 and Config3 only
- Config1, Config2, and Config3

Firefox:
- Config1 only
- Config2 only
- Config1 and Config2 only
- Config2 and Config3 only
- Config1, Config2, and Config3

Hide Answer

Suggested Answer:

by DiegoWill at *April 21, 2025, 9:43 p.m.*

Comments

DiegoWill Highly Voted 7 months, 3 weeks ago

The question is incomplete: where is the configuration information?

upvoted 6 times

Newb007 7 months ago

ya I think it might just be Device 1 and Device 2 (assuming they mean device instead of config) These extensions are only supported on Windows I belive

https://learn.microsoft.com/en-us/training/modules/purview-implement-endpoint-dlp/deploy-purview-extension

https://learn.microsoft.com/en-us/purview/dlp-chrome-get-started

https://learn.microsoft.com/en-us/purview/dlp-firefox-extension-get-started

upvoted 8 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 15 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 15

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 tenant.

You have a database that stores customer details. Each customer has a unique 13-digit identifier that consists of a fixed pattern of numbers and letters.

You need to implement a data loss prevention (DLP) solution that meets the following requirements:

Email messages that contain a single customer identifier can be sent outside your company.

Email messages that contain two or more customer identifiers must be approved by the company's data privacy team.

Which two components should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a sensitivity label

B. a sensitive information type **Most Voted**

C. a DLP policy **Most Voted**

D. a retention label

E. a mail flow rule

Hide Answer

Suggested Answer: *BC*

Community vote distribution

BC (86%) 14%

by CuentaRM10 at *May 27, 2025, 3:08 p.m.*

Comments

CuentaRM10 **Highly Voted** 6 months, 2 weeks ago

Selected Answer: BC

The answers are correct

upvoted 8 times

musketoon1871 **Most Recent** 2 weeks, 6 days ago

Selected Answer: BE

mail flow rule needed

upvoted 1 times

Eltooth 2 months, 2 weeks ago

Selected Answer: BC

B and C are correct answers.

upvoted 1 times

Gtc_ 3 months, 2 weeks ago

Selected Answer: BC

DLP and SIT are correct. You can configure DLP to route for approval if conditions are met.

upvoted 3 times

Jadore 5 months, 3 weeks ago

Selected Answer: BE

no approval action in dlp policy

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 16 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 16

Topic #: 2

[All SC-401 Questions]

DRAG DROP -

You have a Microsoft 365 E5 subscription that has data loss prevention (DLP) implemented.

You need to create a custom sensitive info type. The solution must meet the following requirements:

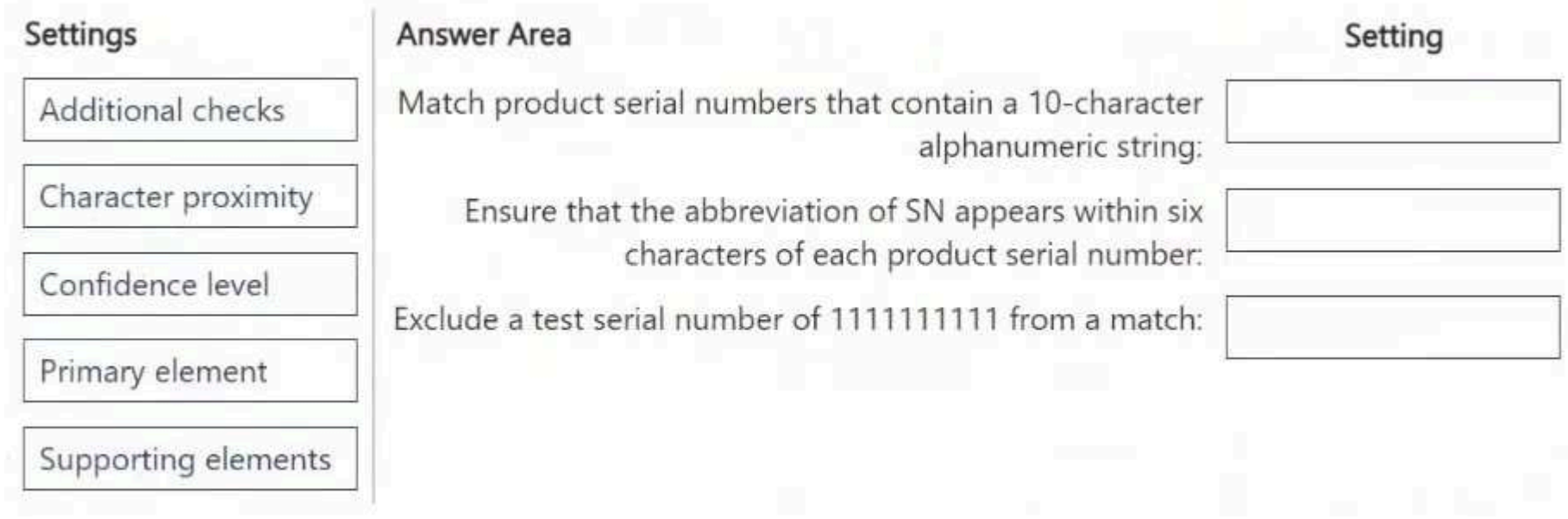
Match product serial numbers that contain a 10-character alphanumeric string.

Ensure that the abbreviation of SN appears within six characters of each product serial number.

Exclude a test serial number of 1111111111 from a match.

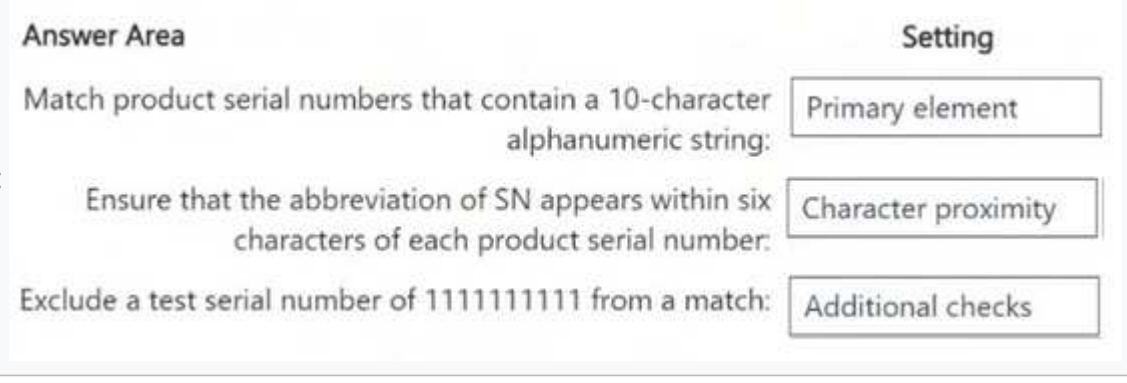
Which pattern settings should you configure for each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.


Settings
Additional checks
Character proximity
Confidence level
Primary element
Supporting elements
Answer Area
Setting
Match product serial numbers that contain a 10-character alphanumeric string:
Ensure that the abbreviation of SN appears within six characters of each product serial number:
Exclude a test serial number of 1111111111 from a match:

Hide Answer

Suggested Answer:


Answer Area
Setting
Match product serial numbers that contain a 10-character alphanumeric string:
Primary element
Ensure that the abbreviation of SN appears within six characters of each product serial number:
Character proximity
Exclude a test serial number of 1111111111 from a match:
Additional checks

by PsiCzar at *June 12, 2025, 5:05 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Primary element
Character proximity
Additional checks

upvoted 2 times

4d76265 6 months ago

Given answers are correct - tested in Purview.

upvoted 4 times

PsiCzar 6 months ago

Correct.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 17 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 17

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription.

You need to prevent users from uploading data loss prevention (DLP)-protected documents to the following third-party websites:

web1.contoso.com web2.contoso.com

The solution must minimize administrative effort.

To what should you set the Service domains setting for Endpoint DLP?

A. *.contoso.com

B. contoso.com

C. web1.contoso.com and web2.contoso.com **Most Voted**

D. web*.contoso.com

Hide Answer

Suggested Answer: *C*

Community vote distribution

C (85%) D (15%)

by Linpus at *May 27, 2025, 5:32 p.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: C

I agree with C - least admin effort and does not block wildcard child domains of contoso.com.

upvoted 1 times

4d76265 6 months ago

Selected Answer: C

D is not possible in Purview.

A is possible but you would be blocking more than intended so you could spend more time allowing other subdomains.

C seems best fit for least admin effort.

upvoted 4 times

58d4802 6 months ago

Selected Answer: C

I agree with option C because it is specifically targeting the two mentioned websites , nothing more nothing less

upvoted 2 times

PsiCzar 6 months, 1 week ago

Selected Answer: C

I'm unable to add web*.contoso.com to the list of service domains in the Endpoint DLP settings of my dev environment. I can type it in, click the + and click Save but it doesnt appear in the list, and I tried multiple times. I am able to add all other domain examples in the answers, but I suspect the correct answer is D, because *.contoso.com and contoso.com are pretty broad answers and would block anything on that domain so would be overkill.

upvoted 4 times

Linpus 6 months, 2 weeks ago

Selected Answer: D

This will match both web1.contoso.com and web2.contoso.com in one rule.

upvoted 2 times

Jol 6 months, 1 week ago

I agree!

upvoted 1 times

papillor 6 months, 1 week ago

I would agree with you, it saves us time when creating but I'd wager they are playing with the "overreaching" factor. Maybe web3.contoso.com is a supported website for upload documents and it would add administrative effort to correct the initial policy. The correct answer is C

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 18 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 18

Topic #: 2

[All SC-401 Questions]

You are creating a data loss prevention (DLP) policy that will apply to all available locations except Fabric and Power BI workspaces.

You configure an advanced DLP rule in the policy.

Which type of condition can you use in the rule?

A. Sensitive info type **Most Voted**

B. Content search query

C. Sensitive label

D. Keywords

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (100%)

by papillor at *June 3, 2025, 5:05 p.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: A

A is correct answer.

upvoted 2 times

gabbinu 3 months, 3 weeks ago

Selected Answer: A

https://learn.microsoft.com/en-us/purview/dlp-sensitivity-label-as-condition
Sensitivity Labels as a condition will not be available if you have selected Teams chat and channel messages as a location to apply the DLP policy.

upvoted 2 times

PsiCzar 6 months, 1 week ago

Selected Answer: A

Correct, tested in my dev environment

upvoted 3 times

papillor 6 months, 1 week ago

Selected Answer: A

Correct answer

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 19 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 19

Topic #: 2

[All SC-401 Questions]

HOTSPOT -

You plan to create a custom sensitive information type that will use Exact Data Match (EDM).

You need to identify what to upload to Microsoft 365, and which tool to use for the upload.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Upload:
- Data hashes
- Data in the XML format
- Digitally signed data

Use:
- Azure Storage Explorer
- EDM upload agent
- Microsoft Purview portal
- The Set-DlpKeywordDictionary cmdlet

Hide Answer

Suggested Answer:

Answer Area

Upload: Data hashes

Use: EDM upload agent

by PsiCzar at *June 5, 2025, 5:08 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Data hashes
EDM Upload Agent

https://learn.microsoft.com/en-us/purview/sit-get-started-exact-data-match-hash-upload?tabs=two-computers

upvoted 2 times

gabbinu 3 months, 3 weeks ago

Data hashes: Only the hashed version of the sensitive data is uploaded
https://learn.microsoft.com/en-us/purview/sit-learn-about-exact-data-match-based-sits

EDM Upload Agent: used to hash, with a salt value, the sensitive information source table, and upload it.
https://learn.microsoft.com/en-us/purview/sit-get-started-exact-data-match-hash-upload

upvoted 1 times

PsiCzar 6 months, 1 week ago

Correct.

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 20 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 20

Topic #: 2

[All SC-401 Questions]

DRAG DROP -

You need to create a trainable classifier that can be used as a condition in an auto-apply retention label policy.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Publish the trainable classifier.	
Retrain the trainable classifier.	
Create the trainable classifier.	
Test the trainable classifier.	
Create a terms of use (ToU) policy.	

Hide Answer

Suggested Answer:

Actions	Answer Area
Retrain the trainable classifier.	Create the trainable classifier.
Create a terms of use (ToU) policy.	Test the trainable classifier.
	Publish the trainable classifier.

by PsiCzar at *June 5, 2025, 5:17 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Create
Test
Publish

upvoted 3 times

PsiCzar 6 months, 1 week ago

Correct. You can no longer retrain a trainable classifier and creating a terms of use policy isnt a thing. The order can be found here https://learn.microsoft.com/en-us/purview/trainable-classifiers-get-started-with

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 21 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 21

Topic #: 2

[All SC-401 Questions]

You have Microsoft 365 E5 subscription that uses data loss prevention (DLP) to protect sensitive information.

You have a document named Form.docx.

You plan to use PowerShell to create a document fingerprint based on Form.docx.

You need to first connect to the subscription.

Which cmdlet should you run?

A. Connect-IPPSSession **Most Voted**

B. Connect-SPOService

C. Connect-ExchangeOnline

D. Connect-MgGraph

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (100%)

by 4d76265 at *June 12, 2025, 1:44 p.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: A

A is correct answer.

https://learn.microsoft.com/en-us/powershell/module/exchangepowershell/new-dlpfingerprint?view=exchange-ps

https://learn.microsoft.com/en-us/powershell/exchange/connect-to-scc-powershell?view=exchange-ps

upvoted 3 times

gabbinu 3 months, 3 weeks ago

Selected Answer: A

you must first connect to the Security & Compliance Center through Connect-IPPSSession

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 22 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 22

Topic #: 2

[All SC-401 Questions]

You receive an email that contains a list of words that will be used for a sensitive information type.

You need to create a file that can be used as the source of a keyword dictionary.

In which format should you save the list?

A. an XLSX file that contains one word in each cell of the first row

B. an XML file that contains a keyword tag for each word

C. an ACCDB database file that contains a table named Dictionary

D. a text file that has one word on each line **Most Voted**

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (100%)

by 4d76265 at *June 12, 2025, 1:47 p.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: D

D is correct answer.

https://learn.microsoft.com/en-us/purview/sit-create-a-keyword-dictionary#basic-steps-to-creating-a-keyword-dictionary

upvoted 3 times

gabbinu 3 months, 3 weeks ago

Selected Answer: D

When you create a keyword dictionary for a Sensitive Information Type (SIT) in Microsoft Purview, copy your keywords into a text file and make sure that each keyword is on a separate line.

upvoted 2 times

ppolychron 4 months, 1 week ago

Selected Answer: D

Most commonly you compile your keywords for your dictionary in a file, such as a .csv or .txt list.
https://learn.microsoft.com/en-us/purview/sit-create-a-keyword-dictionary#basic-steps-to-creating-a-keyword-dictionary

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 23 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 23
Topic #: 2
[All SC-401 Questions]

Your company has a Microsoft 365 tenant.
The company performs annual employee assessments. The assessment results are recorded in a document named AssessmentTemplate.docx that is created by using a Microsoft Word template. Copies of the employee assessments are sent to employees and their managers.
The assessment copies are stored in mailboxes, Microsoft SharePoint Online sites, and OneDrive folders. A copy of each assessment is also stored in a SharePoint Online folder named Assessments.
You need to create a data loss prevention (DLP) policy that prevents the employee assessments from being emailed to external users. You will use a document fingerprint to identify the assessment documents. The solution must minimize effort.
What should you include in the solution?

A. Create a fingerprint of AssessmentTemplate.docx. **Most Voted**

B. Create a sensitive info type that uses Exact Data Match (EDM).

C. Import 100 sample documents from the Assessments folder to a seed folder.

D. Create a fingerprint of 100 sample documents in the Assessments folder.

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (100%)

by 4d76265 at *June 12, 2025, 1:50 p.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: A

A is correct answer.

upvoted 1 times

deeptha92 3 months, 2 weeks ago

Selected Answer: A

CHAT GPT answer

Answer: A — Create a fingerprint of AssessmentTemplate.docx.

Reason: Document fingerprinting is designed for form-based files created from a common template. Since every assessment is produced from the same Word template, uploading that template as the fingerprint lets your DLP policy detect and block those assessments with the least effort.

upvoted 3 times

Jdr379 5 months, 2 weeks ago

Selected Answer: A

Agree with A

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 24 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 24

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that uses Microsoft Purview.

You are creating an exact data match (EDM) classifier named EDM1.

For EDM1, you upload a schema file that contains the fields shown in the following table.

Column name	Match mode
PP	EU Passport Number
Name	All Full Names
DateOfBirth	Single-token
AccountNumber	Multi-token

What is the maximum number of primary elements that EDM1 can have?

A. 1

B. 2

C. 3

D. 4 **Most Voted**

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (80%) C (16%) 4%

by 58d4802 at *June 11, 2025, 5:20 a.m.*

Comments

7259dc7 **Highly Voted** 5 months ago

Selected Answer: D

According to the latest updates.
At least 1 and maximum 10 primary elements

upvoted 7 times

PsiCzar **Highly Voted** 6 months ago

Selected Answer: D

Incorrect. In the EDM wizard of my dev environment it states you can select up to 10 primary elements, I created an EDM classifier with 4 columns like the question and I could select all 4 as a primary element, click Next and finish the wizard without error. So the answer is D. 4.

upvoted 5 times

Eltooth Most Recent 2 months, 2 weeks ago

Selected Answer: D

D is correct answer : 4

However, For each EDM SIT, you must select at least one primary element and no more than 10 primary elements.

https://learn.microsoft.com/en-us/purview/sit-create-edm-sit-unified-ux-schema-rule-package

upvoted 3 times

454252dfr 4 months, 1 week ago

Selected Answer: C

The maximum number of primary elements that an EDM classifier can have is 3, when using a composite primary key.

upvoted 2 times

zied01 4 months, 3 weeks ago

Selected Answer: B

the supporting elements are relative to SIT , we can't make a column as primary element without link to a sit , in the table of the question , there is only two SIT , so the correct answer is 2

we can't make a column as a primary element if this colum is single or multiple token

upvoted 1 times

7259dc7 5 months, 3 weeks ago

Selected Answer: D

Incorrect.
The maximum number of primary elements an Exact Data Match (EDM) classifier can have is 10, according to Microsoft Learn.
When creating an EDM sensitive information type (SIT), you must select at least one primary element and can select up to ten.

upvoted 5 times

58d4802 6 months ago

Selected Answer: C

Correct answer is C because You can choose up to 3 primary fields, but only one of them can be multi-token. So, valid primary combinations include:
Full name (multi-token) + Passport number + Date of birth
or
Account number (multi-token) + Passport number + Date of birth

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 25 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 25

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that contains a trainable classifier named Trainable1.

You plan to create the items shown in the following table.

Name	Type
Label1	Sensitivity label
Label2	Retention label
Policy1	Retention label policy
DLP1	Data loss prevention (DLP) policy

Which items can use Trainable 1?

A. Label2 only

B. Label1 and Label2 only

C. Label1 and Policy1 only

D. Label2, Policy1, and DLP1 only

E. Label1, Label2, Policy1, and DLP1 **Most Voted**

Hide Answer

Suggested Answer: *E*

Community vote distribution

E (58%) D (42%)

by SH_Train at *June 5, 2025, 12:42 a.m.*

Comments

SH_Train **Highly Voted** 6 months, 1 week ago

Selected Answer: E

Answer should be Label1, Policy1, DLP1. Retention Labels do not use Trainable Classifiers, but you can apply a Retention Label via a Retention Policy that uses a Trainable Classifier.

upvoted 9 times

Ender3 **Most Recent** 2 months ago

Selected Answer: E

I voted E, like others did, not because it is correct but because a vote is required to submit a comment. I think we can all agree that all answers are wrong as of October 2025. I went through and tested each case and can confirm the following:

Label1: Sensitivity Label - Yes
Label2: Retention Label - No
Policy1: Retention Lable Policy - Yes
DLP1: DLP Policy - Yes

It should be noted that during the creation process of a sensitivity label, you get the option to configure an auto-labeling rule. This rule applies only in Office applications when users create/edit documents (so it's client side), and it is different from configuring an auto-labeling policy.

upvoted 1 times

Eltooth 2 months, 2 weeks ago

Selected Answer: E

E is correct answer.
Label 1
Policy 1
DLP 1

https://learn.microsoft.com/en-us/purview/trainable-classifiers-learn-about#where-you-can-use-classifiers

upvoted 1 times

Eltooth 2 months, 2 weeks ago

And Retention 1

upvoted 1 times

Caezarlay 2 months, 2 weeks ago

Selected Answer: D

Retention labels → ✅ You can configure a retention label to auto-apply based on a classifier.

Retention label policies → These publish the label, and classifiers help determine where the label applies.

DLP policies → Classifiers can be used as conditions to trigger DLP actions.

Sensitivity labels → ❌ These do not support trainable classifiers. They rely on manual application, sensitive info types, or auto-labeling rules—not classifiers.

upvoted 1 times

Eltooth 2 months, 2 weeks ago

https://learn.microsoft.com/en-us/purview/trainable-classifiers-learn-about#where-you-can-use-classifiers

upvoted 1 times

gabbinu 3 months, 3 weeks ago

Selected Answer: E

Correct Answer:
E. Label1, Policy1, and DLP1

Sensitivity labels (Label1)
Yes → you can auto-apply sensitivity labels using trainable classifiers.

Retention labels (Label2)
Wrong → Trainable classifiers cannot be directly applied to retention labels themselves.
They can only be used in auto-apply retention label policies (Policy1).

Retention label policy (Policy1)
Yes → You can create an auto-apply retention label policy based on trainable classifiers.

DLP policy (DLP1)
Yes → Trainable classifiers can be conditions in Microsoft Purview DLP policies.

upvoted 3 times

gabbinu 3 months, 3 weeks ago

Sorry, correct answer should be Label1, Policy1, and DLP1.
Instead E. says Label1, Label2, Policy1, and DLP1

upvoted 1 times

DrArjunReddy 4 months, 2 weeks ago

Selected Answer: D

The answer is Policy 1 and DLP 1. There is no option of applying TC to Sensitivity label or ret label. Once you create labels, you can apply TC based scoping to the auto sensitivity or ret policies but not the label itself

upvoted 2 times

Leon1969 1 month, 3 weeks ago

In my opinion this is the only correct answer because you can only use trainable classifiers in polices, not in labels themselves.

upvoted 1 times

zied01 5 months, 1 week ago

Selected Answer: D

how can we use a Trainable classifier with a senstive label (except the auto label policy..) !!!!!

upvoted 3 times

Jdr379 5 months, 2 weeks ago

Selected Answer: D

Answer is D. Look at SC-400 exam questions. Q30 Topic 3. Same question and E is not an option on it.

upvoted 3 times

Jadore 5 months, 3 weeks ago

Selected Answer: D

Ret label does not use TC

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 26 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 26

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 E5 tenant.

You need to add a new keyword dictionary.

What should you create?

A. a trainable classifier

B. a retention policy

C. a sensitivity label

D. a sensitive info type **Most Voted**

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (100%)

by 4d76265 at *June 12, 2025, 2:02 p.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: D

The correct answer is: D. a sensitive info type.
To add a new keyword dictionary in a Microsoft 365 E5 tenant, you need to create a custom sensitive information type. Keyword dictionaries are used within sensitive info types to define patterns or terms that should be detected in content (e.g., emails, documents).
This is commonly used in Data Loss Prevention (DLP) policies and Microsoft Purview solutions to identify and protect sensitive data.
Here's a quick breakdown of the other options:
A. Trainable classifier: Used for identifying content based on machine learning, not keyword dictionaries.
B. Retention policy: Manages data lifecycle, not detection of keywords.
C. Sensitivity label: Applies protection like encryption or access control, but doesn't define keyword detection.

upvoted 2 times

4d76265 6 months ago

Selected Answer: D

Given answer is correct. Keyword dictionary is available with a SIT.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 27 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 27

Topic #: 2

[All SC-401 Questions]

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 tenant and 500 computers that run Windows 11. The computers are onboarded to Microsoft Purview.
You discover that a third-party application named Tailspin_scanner.exe accessed protected sensitive information on multiple computers.
Tailspin_scanner.exe is installed locally on the computers.
You need to block Tailspin_scanner.exe from accessing sensitive documents without preventing the application from accessing other documents.
Solution: From the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings, you add a folder path to the file path exclusions.
Does this meet the goal?

A. Yes

B. No **Most Voted**

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (100%)

by 4d76265 at *June 12, 2025, 2:06 p.m.*

Comments

mlstud 5 days, 18 hours ago

Selected Answer: B

No, that does not meet the goal.
Adding a folder path to file path exclusions in Endpoint DLP will exclude that folder from DLP monitoring, meaning sensitive documents in that path will no longer be protected. This is the opposite of what you want because it reduces protection rather than blocking Tailspin_scanner.exe.

upvoted 1 times

Eltooth 2 months, 2 weeks ago

Selected Answer: B

No is correct answer.

upvoted 3 times

4d76265 6 months ago

Selected Answer: B

Given answer is correct. If you add a file path exclusion, you are allowing access, not blocking it from accessing sensitive documents.

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 28 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 28

Topic #: 2

[All SC-401 Questions]

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 tenant and 500 computers that run Windows 11. The computers are onboarded to Microsoft Purview.
You discover that a third-party application named Tailspin_scanner.exe accessed protected sensitive information on multiple computers.
Tailspin_scanner.exe is installed locally on the computers.
You need to block Tailspin_scanner.exe from accessing sensitive documents without preventing the application from accessing other documents.
Solution: From Microsoft Defender for Cloud Apps, you create an app discovery policy.
Does this meet the goal?

A. Yes

B. No **Most Voted**

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (100%)

by 4d76265 at *June 12, 2025, 2:09 p.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: B

B is correct answer: No

upvoted 1 times

4d76265 6 months ago

Selected Answer: B

Given answer is correct. A Defender app discovery policy monitors and logs but does not block and does not control local executables.

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 29 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 29
Topic #: 2
[All SC-401 Questions]

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 tenant and 500 computers that run Windows 11. The computers are onboarded to Microsoft Purview.
You discover that a third-party application named Tailspin_scanner.exe accessed protected sensitive information on multiple computers.
Tailspin_scanner.exe is installed locally on the computers.
You need to block Tailspin_scanner.exe from accessing sensitive documents without preventing the application from accessing other documents.
Solution: From the Microsoft Defender for Cloud Apps, you mark the application as Unsanctioned.
Does this meet the goal?

A. Yes

B. No **Most Voted**

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (100%)

by 4d76265 at *June 12, 2025, 2:12 p.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: B

B is correct answer: No

upvoted 1 times

4d76265 6 months ago

Selected Answer: B

Given answer is correct. Marking an app as "unsanctioned" means you've flagged the app for further monitoring but does not block and does not control local executables.

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 30 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 30

Topic #: 2

[All SC-401 Questions]

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You recently discovered that the developers at your company emailed Azure Storage Account keys in plain text to third parties.
You need to ensure that when Azure Storage Account keys are emailed, the emails are encrypted.
Solution: You configure a mail flow rule that matches a sensitive info type.
Does this meet the goal?

A. Yes **Most Voted**

B. No

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (70%) B (30%)

by Jarem at *June 10, 2025, 6:53 p.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: A

A. Yes, this solution does meet the goal.

By configuring a mail flow rule that matches a sensitive info type—such as Azure Storage Account keys—you can automatically apply email encryption when such content is detected. Microsoft 365 includes built-in sensitive information types, and you can also create custom ones to match specific patterns like storage keys.

Why this works:
Sensitive info types allow for precise detection of confidential data.
Mail flow rules can be configured to encrypt emails, redirect, or block them based on matches.
This approach is automated and scalable, reducing the risk of human error.

upvoted 1 times

ppolychron 4 months, 1 week ago

Selected Answer: B

Microsoft has stopped supporting DLP-related rules in Exchange Online Transport Rules. The option is no longer available.

Answer is NO.

https://techcommunity.microsoft.com/blog/exchange/exchange-online-mail-flow-rules-to-stop-supporting-dlp-related-rules-conditions-/3959870

upvoted 3 times

58d4802 6 months ago

Selected Answer: A

Microsoft Purview includes built-in sensitive info types, including one for Azure Storage Account keys. You can create a mail flow rule (also known as a transport rule) in Exchange that:
Detects this sensitive info type in the message body or attachments
Automatically applies encryption (e.g., Microsoft Purview Message Encryption)

upvoted 3 times

zied01 5 months ago

hello
i can't see the setting relative to the SIT in the mail transport rule assistant in Exchange admin center

upvoted 2 times

shaunshauncybersecchecke 6 months ago

Selected Answer: A

The mail flow rule should automatically apply nessacry encryption

upvoted 1 times

Mushroomski 6 months ago

Selected Answer: A

The mail flow rule that matches the Azure Storage Account Key sensitive info type and applies encryption (like OME) does meet the goal — assuming it's configured with the correct conditions and actions.

upvoted 1 times

Jarem 6 months ago

Selected Answer: A

Yes, this solution meets the goal. By configuring a mail flow rule that matches a sensitive info type, you can ensure that emails containing Azure Storage Account keys are encrypted. This rule can detect when sensitive information is being sent and apply encryption to protect the data.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 31 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 31

Topic #: 2

[All SC-401 Questions]

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You recently discovered that the developers at your company emailed Azure Storage Account keys in plain text to third parties.
You need to ensure that when Azure Storage Account keys are emailed, the emails are encrypted.
Solution: You create a data loss prevention (DLP) policy that has only the Exchange email location selected.
Does this meet the goal?

A. Yes **Most Voted**

B. No

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (63%) B (37%)

by dache at *June 7, 2025, 10:21 a.m.*

Comments

4d76265 **Highly Voted** 6 months ago

Selected Answer: A

Given answer is correct. I have tested in Purview - I can create new DLP policy > scope to Exchange > content contains built-in SIT for Azure Storage Account Keys > restrict or encrypt the content in 365 locations > choose protection setting for encryption. Test, test, test, and don't rely solely on Copilot.

upvoted 8 times

dache **Highly Voted** 6 months, 1 week ago

Selected Answer: B

Copilot:
The correct answer is: B. No.
A DLP policy with only the Exchange email location selected can detect and restrict the sharing of Azure Storage Account keys, but it does not automatically encrypt emails. To ensure encryption, you need to configure Microsoft Purview Information Protection or Microsoft Defender for Office 365 to enforce encryption policies when sensitive data is detected.

upvoted 6 times

Alcpt Most Recent 1 month ago

Selected Answer: B

B
No, selecting only the Exchange email location in a data loss prevention (DLP) policy is not enough to encrypt emails on its own; you must also configure a specific action within the policy to enforce encryption. This question says nothing about making additional / complete DLP configs.

upvoted 1 times

Eltooth 2 months, 2 weeks ago

Selected Answer: A

A. Yes, this solution does meet the goal — assuming the DLP policy is properly configured.

By creating a Data Loss Prevention (DLP) policy that targets Exchange email and includes rules to detect Azure Storage Account keys, you can enforce email encryption when such sensitive information is found. This helps prevent the transmission of secrets in plain text.

Key Considerations:
The DLP policy must include accurate pattern matching for Azure Storage Account keys (e.g., using regular expressions or sensitive info types).
The policy action must be set to encrypt the email or apply other protective measures.
Since the location is set to Exchange email only, it will not cover other channels like Teams or SharePoint — but for email-specific protection, this is sufficient.

upvoted 2 times

almitite 4 months, 1 week ago

Selected Answer: A

The DLP policy can then automatically enforce actions, such as encrypting the email, blocking it, or displaying warnings.

upvoted 1 times

ppolychron 4 months, 1 week ago

Selected Answer: A

Answer Is Correct.

Create a new DLP Policy with Exchange as location and Select:
Conditions
Content is shared from Microsoft 365 with people outside my organization
AND
Content contains-> sensitive information types> Azure Storage Account Key
Actions
Restrict access or encrypt the content in Microsoft 365 locations ->Encrypt email messages - > Select Encrypt (This is an OME template, you can also select a sensitivity label)

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 32 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 32

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 E5 tenant and the Windows Client devices shown in the following table.

Name	Joined to Microsoft Entra	Configuration
Device1	Yes	Onboarded to Microsoft Purview
Device2	Yes	Onboarded to Microsoft Defender for Endpoint
Device3	Yes	Enrolled in Microsoft Intune
Device4	No	Enrolled in Microsoft Intune

To which devices can you apply Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings?

A. Device1 only **Most Voted**

B. Device1 and Device2 only

C. Device1 and Device3 only

D. Device1, Device3, and Device4 only

E. Device1, Device2, Device3, and Device4

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:13 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: A

A is correct answer :Device 1 only.
Reason:
Devices that are Entra ID joined (or hybrid joined)
Devices that are onboarded to Microsoft Purview

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 33 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 33

Topic #: 2

[All SC-401 Questions]

HOTSPOT

-

You plan to implement Microsoft 365 Endpoint data loss prevention (Endpoint DLP).

You need to identify which end user activities can be audited on the endpoints, and which activities can be restricted on the endpoints.

What should you identify for each activity? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

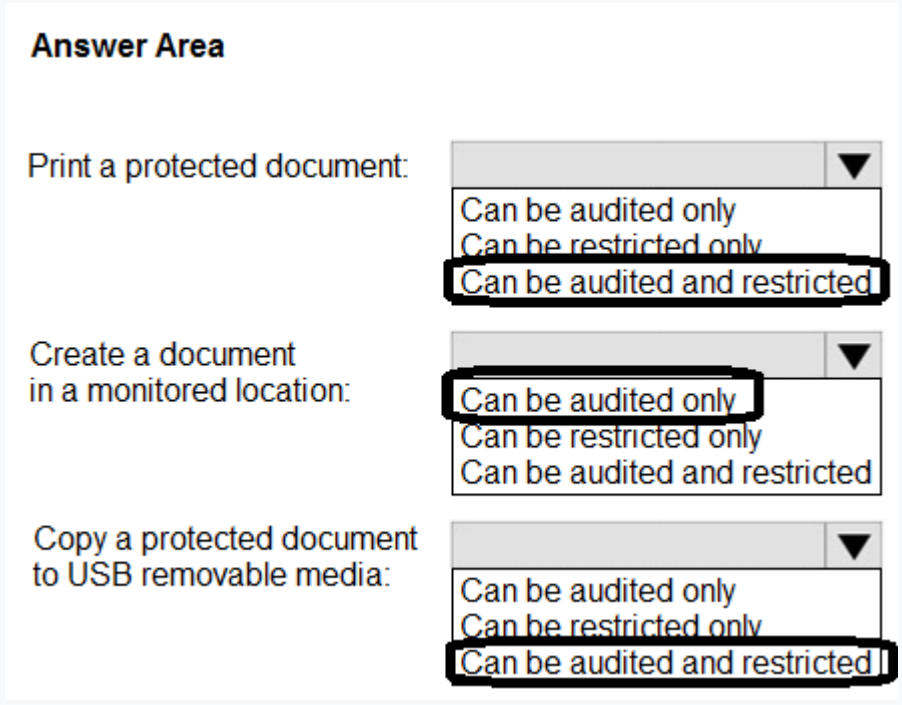
Print a protected document:
- Can be audited only
- Can be restricted only
- Can be audited and restricted

Create a document in a monitored location:
- Can be audited only
- Can be restricted only
- Can be audited and restricted

Copy a protected document to USB removable media:
- Can be audited only
- Can be restricted only
- Can be audited and restricted

Hide Answer

Suggested Answer:


Answer Area
Print a protected document:
Can be audited only
Can be restricted only
Can be audited and restricted
Create a document in a monitored location:
Can be audited only
Can be restricted only
Can be audited and restricted
Copy a protected document to USB removable media:
Can be audited only
Can be restricted only
Can be audited and restricted

by Seidor_Analytics at *Sept. 5, 2025, 8:14 a.m.*

Comments

Eltooth 2 months, 1 week ago

Answer is correct:
Print - Audited and restricted
Create - Audited Only
Copy - Audited and restricted

upvoted 2 times

RickySmith 2 months, 2 weeks ago

Print - Audited and restricted
Create - Audited
Copy - Audited and restricted
https://learn.microsoft.com/en-us/purview/endpoint-dlp-learn-about?preserve-view=true&view=o365-worldwide#endpoint-activities-you-can-monitor-and-take-action-on

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 34 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 34

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that contains a data loss prevention (DLP) policy named DLP1. DLP1 contains the DLP rules shown in the table.

Name	Priority	User notifications	Policy tip	If there's a match for this rule, stop processing additional DLP policies and rules
Rule1	0	On	Tip 1	Enabled
Rule2	1	On	Tip 2	Enabled
Rule3	2	On	Tip 3	Disabled
Rule4	3	On	Tip 4	Enabled

You need to ensure that when a document matches all the rules, users will see Tip 2.

What should you change?

A. the priority setting of Rule2 to 0 **Most Voted**

B. the priority setting of Rule2 to 2

C. the priority setting of Rule3 and Rule4 to 0

D. the if there's a match for this rule, stop processing additional DLP policies and rules setting for Rule3 to Enabled

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:14 a.m.*

Comments

Eltooth Highly Voted 2 months, 2 weeks ago

Selected Answer: A

A is correct answer: Change priority setting of rule 2 to 0 (move all other down).
Note: The lower the number, the higher the priority i.e. Priority 0 wins over priority 1, 2 3 etc.

upvoted 5 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 35 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 35

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 E5 tenant that contains the policies shown in the following table.

Name	Type	Retention period	Start the retention period based on	At the end of the retention period
Label1	Label	5 years	When items were created	Delete items automatically
Label2	Retention	7 years	When items were created	Delete items automatically
Labe3	Retention	10 years	When items were created	Do nothing

A file named File1 has all the policies applied.

How long will File1 be retained?

A. File1 will be deleted automatically after 10 years.

B. File1 will be deleted automatically after five years.

C. File1 will be retained until the file is deleted manually. **Most Voted**

D. File1 will be deleted automatically after seven years.

Hide Answer

Suggested Answer: *C*

Community vote distribution

C (55%) A (45%)

by Seidor_Analytics at *Sept. 5, 2025, 8:15 a.m.*

Comments

5840b27 **Highly Voted** 1 month ago

Selected Answer: A

Microsoft retention handles retention and deletion separately. The longest retention wins so retained for 10 years. The delete action of the other retention policy and label is suspended during this time, but at the end of the 10-year retention period, the file will be deleted.

https://learn.microsoft.com/en-us/purview/retention?tabs=table-overriden#the-principles-of-retention-or-what-takes-precedence

upvoted 5 times

Eltooth Most Recent 2 months, 2 weeks ago

Selected Answer: C

Longest retention wins (10 years) and since no auto-delete is configured, file will be retained until manually deleted.

upvoted 3 times

Caezarlay 2 months, 3 weeks ago

Selected Answer: C

According to principle of retention, it will last for 10 years and it will not be deleted automatically.

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 36 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 36

Topic #: 2

[All SC-401 Questions]

You have a Microsoft SharePoint Online site named Site1 that contains the files shown in the following table.

Name	Number of IP addresses in the file
File1	2
File2	3

You have a data loss prevention (DLP) policy named DLP1 that has the advanced DLP rules shown in the following table.

Name	Content contains	Policy tip	If match, stop processing	Priority
Rule1	1 or more IP addresses	Tip1	No	0
Rule2	3 or more IP addresses	Tip2	Yes	1
Rule3	2 or more IP addresses	Tip3	No	2

You apply DLP1 to Site1.

Which policy tips will appear for File2?

A. Tip1 only

B. Tip2 only

C. Tip3 only

D. Tip1 and Tip2 only **Most Voted**

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:14 a.m.*

Comments

skalolaz Highly Voted 3 months, 1 week ago

Selected Answer: D

Rules 1 and 2 match the number of IP addresses.

upvoted 6 times

Eltooth Most Recent 2 months, 1 week ago

Selected Answer: D

D is correct answer: Tip1 and Tip2 and Rule 1 has 0 priority, which is highest/first, then rule 2 stops processing.

upvoted 2 times

Caezarlay 2 months, 2 weeks ago

Selected Answer: D

D. Tip1 and Tip2 only

Both rules match and both tips will be shown since processing continues through all rules.

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 37 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 37

Topic #: 2

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft SharePoint Online site named Site1 that has the users shown in the following table.

Name	Role
User1	Owner
User2	Member

You create the retention labels shown in the following table.

Name	Retention period	Retention action	Based on
Retention1	4 years	Retain only	When a file was labeled
Retention2	2 years	Retain and delete	When a file was labeled

You publish the retention labels to Site1.

On March 1, 2023, you assign the retention labels to the files shown in the following table.

Name	Modified by	Retention label
File1	User1	Retention1
File2	User1	Retention2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
User1 can delete File1 on March 10, 2023.	○	○
User2 can delete File1 on March 10, 2027.	○	○
User2 can edit File2 on March 15, 2025.	○	○

Hide Answer

Suggested Answer:

Answer Area

Statements	Yes	No
User1 can delete File1 on March 10, 2023.	○	●
User2 can delete File1 on March 10, 2027.	●	○
User2 can edit File2 on March 15, 2025.	●	○

by Seidor_Analytics at *Sept. 5, 2025, 8:15 a.m.*

Comments

RickySmith Highly Voted 3 months ago

Y - User can delete, but it goes into Preservation Hold - https://learn.microsoft.com/en-us/purview/retention-policies-sharepoint#how-retention-works-for-sharepoint-and-onedrive
Y - If the above was not done then Yes, else No because the file is already in Preservation Hold
N - File is already deleted as per Retention2

upvoted 7 times

florinvele Most Recent 2 months, 4 weeks ago

1. User1 can delete File1 on March 10, 2023.

File1 has Retention1 (Retain only, 4 years).

Until 2027, deletion is blocked (even for owners).

Answer: No

2. User2 can delete File1 on March 10, 2027.

Retention1 keeps File1 until 4 years after labeling (March 1, 2027).

After March 1, 2027, deletion is allowed.

On March 10, 2027, deletion is possible.

Answer: Yes

3. User2 can edit File2 on March 15, 2023.

File2 has Retention2 (Retain and delete, 2 years).

During the retention period, editing is allowed.

File will be auto-deleted after 2 years (March 1, 2025).

Answer: Yes

upvoted 2 times

QuwQuw 2 months, 3 weeks ago

This is incorrect, its YYN. You got the dates wrong.

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 38 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 38

Topic #: 2

[All SC-401 Questions]

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You implement Microsoft 365 Endpoint data loss prevention (Endpoint DLP).

You have computers that run Windows 11 and have Microsoft 365 Apps installed. The computers are joined to a Microsoft Entra tenant.

You need to ensure that Endpoint DLP policies can protect content on the computers.

Solution: You deploy the Microsoft Purview Information Protection client to the computers.

Does this meet the goal?

A. Yes

B. No **Most Voted**

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:14 a.m.*

Comments

Eltooth 2 months ago

Selected Answer: B

No is correct answer:
To ensure Endpoint DLP policies can protect content on enrolled computers, the following conditions must be met:

Microsoft 365 E5 or equivalent licensing (includes Microsoft Purview DLP).
Windows 10/11 devices must be:

1. Joined to Microsoft Entra ID (formerly Azure AD).
2. Intune-enrolled or onboarded to Microsoft Defender for Endpoint.
3. Microsoft Purview Information Protection client is not required for Endpoint DLP — it's used for labeling and classification, not for enforcing Endpoint DLP policies.
4. Microsoft Purview DLP policies must be configured and assigned to device groups.

upvoted 3 times

Eltooth 2 months, 1 week ago

Selected Answer: B

No is correct answer.
Admin removed my previous answers!

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 39 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 39
Topic #: 2
[All SC-401 Questions]

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You implement Microsoft 365 Endpoint data loss prevention (Endpoint DLP).

You have computers that run Windows 11 and have Microsoft 365 Apps installed. The computers are joined to a Microsoft Entra tenant.

You need to ensure that Endpoint DLP policies can protect content on the computers.

Solution: You enroll the computer in Microsoft Intune.

Does this meet the goal?

A. Yes

B. No **Most Voted**

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:15 a.m.*

Comments

Eltooth 2 months, 1 week ago

Selected Answer: B

B is correct answer.
To meet the goal, you need to:

Onboard devices to Microsoft Defender for Endpoint.
Enable Endpoint DLP in the compliance portal.
Configure and assign Endpoint DLP policies.

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 40 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 40
Topic #: 2
[All SC-401 Questions]

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You implement Microsoft 365 Endpoint data loss prevention (Endpoint DLP).

You have computers that run Windows 11 and have Microsoft 365 Apps installed. The computers are joined to a Microsoft Entra tenant.

You need to ensure that Endpoint DLP policies can protect content on the computers.

Solution: You deploy the Endpoint DLP configuration package to the computers.

Does this meet the goal?

A. Yes **Most Voted**

B. No

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:13 a.m.*

Comments

Eltooth 2 months, 1 week ago

Selected Answer: A

Correct answer: A. Yes
Deploying the Endpoint DLP configuration package to the computers does meet the goal of enabling Endpoint DLP policies to protect

content.
Here's why:
The Endpoint DLP configuration package is used to onboard devices to Microsoft Defender for Endpoint, which is a required step for Endpoint DLP to function. Once onboarded:

The device can be monitored by Microsoft Purview DLP.
Endpoint DLP policies can be applied to protect sensitive content.
Activities like copying to USB, printing, or uploading to cloud services can be audited or restricted.

Additional Requirements (which you already meet):

Windows 11
Microsoft 365 Apps
Devices joined to Microsoft Entra ID

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 41 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 41

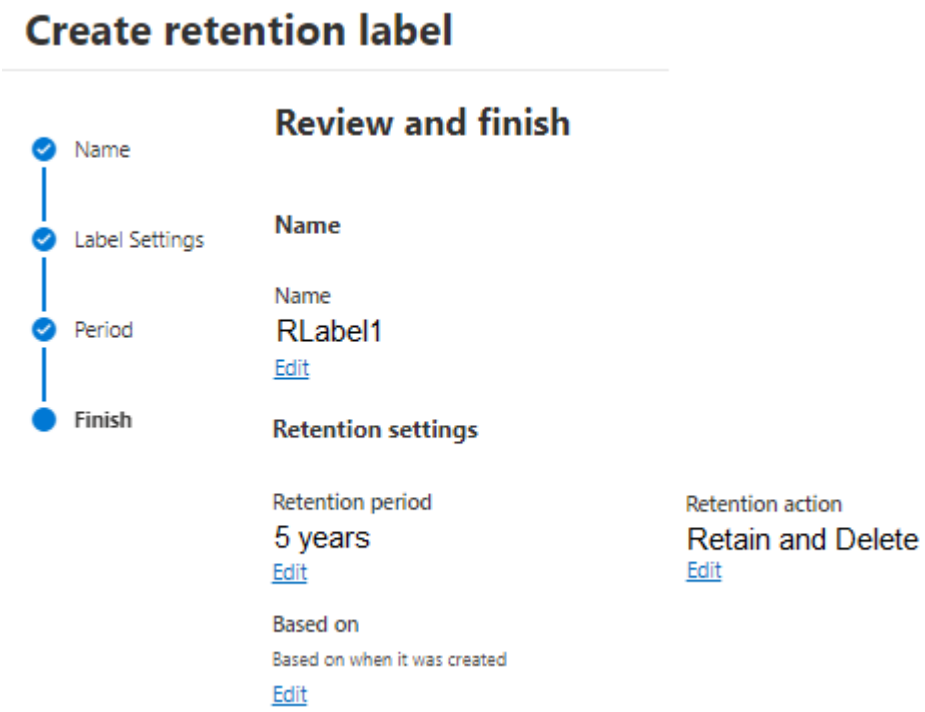
Topic #: 2

[All SC-401 Questions]

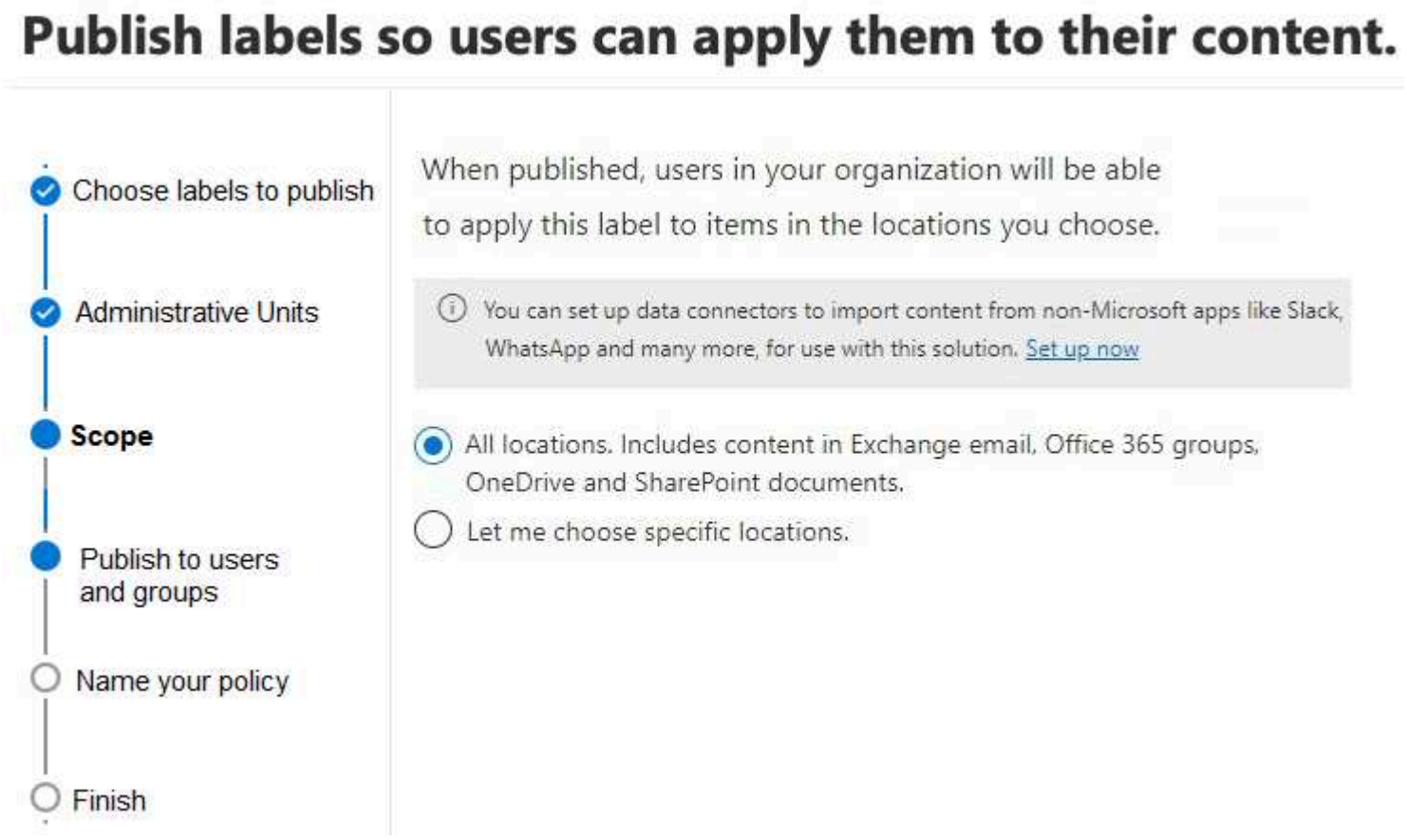
You have a Microsoft 365 E5 subscription that contains the resources shown in the following table.

Name	Type	Location
Mail1	Email message	Microsoft Exchange Online
File1.docx	File	Microsoft SharePoint Online
File2.docx	File	Microsoft OneDrive

You have a retention label configured as shown in the following exhibit.



You publish the retention label and set the scope as shown in the following exhibit.


Publish labels so users can apply them to their content.
Choose labels to publish
Administrative Units
Scope
Publish to users and groups
Name your policy
Finish
When published, users in your organization will be able to apply this label to items in the locations you choose.
You can set up data connectors to import content from non-Microsoft apps like Slack, WhatsApp and many more, for use with this solution. Set up now
All locations. Includes content in Exchange email, Office 365 groups, OneDrive and SharePoint documents.
Let me choose specific locations.

You apply the label to the resources.

Which items can you delete?

A. Mail1 only

B. File1.docx and File2.xlsx only

C. Mail1 and File1.docx only

D. Mail1 and File2.xlsx only

E. Mail1, File1.docx, and File2.xlsx **Most Voted**

Hide Answer

Suggested Answer: *E*

Community vote distribution

E (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:13 a.m.*

Comments

Eltooth 2 months, 1 week ago

Selected Answer: E

E is correct answer.

When a Microsoft 365 retention label policy is applied to All locations, including:
Exchange email
Microsoft 365 Groups
OneDrive
SharePoint
...the ability to delete items depends on the configuration of the retention label itself.
Key Scenarios:
Items that can be deleted after retention period (if label is configured to delete):
Exchange email messages (in user mailboxes and group mailboxes)
OneDrive files and folders
SharePoint documents and list items
Microsoft 365 Group content (e.g., group mailbox items, files in group-connected SharePoint sites).
These items will be automatically deleted after the retention period if the label is configured to "Delete items automatically after retention period ends."

upvoted 1 times

RickySmith 3 months ago

Selected Answer: E

https://learn.microsoft.com/en-us/purview/retention-policies-sharepoint
https://learn.microsoft.com/en-us/purview/retention-policies-exchange

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 42 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 42

Topic #: 2

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 E5 tenant that contains the objects shown in the following table.

Name	Type
Project1	Microsoft Teams team
Sales	Microsoft Teams channel
User1	User

You need to restore a Microsoft Word document that was deleted from the Sales channel by User1.

From where can the document be restored, and how long will the document be retained if it is NOT restored? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

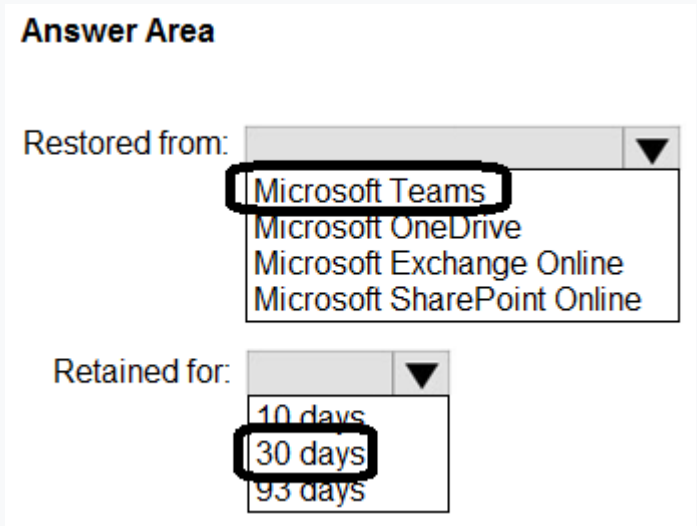
Answer Area

Restored from:
- Microsoft Teams
- Microsoft OneDrive
- Microsoft Exchange Online
- Microsoft SharePoint Online

Retained for:
- 10 days
- 30 days
- 93 days

Hide Answer

Suggested Answer:



by Seidor_Analytics at *Sept. 5, 2025, 8:14 a.m.*

Comments

skalolaz Highly Voted 3 months, 1 week ago

SPO & 93.

upvoted 6 times

Gtc_ 2 months, 3 weeks ago

This is correct. Key part of question is saying it's not restored, so it's just sitting there and that default is 93 days.

upvoted 3 times

Caezarlay Highly Voted 2 months, 2 weeks ago

Restored from: Microsoft SharePoint Online
Retained for: 93 days

upvoted 5 times

RickySmith Most Recent 3 months ago

SPO & 30. 30 is default

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 43 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 43
Topic #: 2
[All SC-401 Questions]

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You implement Microsoft 365 Endpoint data loss prevention (Endpoint DLP).

You have computers that run Windows 11 and have Microsoft 365 Apps installed. The computers are joined to a Microsoft Entra tenant.

You need to ensure that Endpoint DLP policies can protect content on the computers.

Solution: You onboard the computers to Microsoft Defender for Endpoint.

Does this meet the goal?

A. Yes **Most Voted**

B. No

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (83%) B (17%)

by Seidor_Analytics at *Sept. 5, 2025, 8:14 a.m.*

Comments

Alcpt 1 week, 1 day ago

Selected Answer: B

Onboarding to Microsoft Defender for Endpoint alone does not enable Endpoint DLP.
While Defender for Endpoint provides the underlying sensor infrastructure, enabling Endpoint DLP requires additional configuration

within the Microsoft Purview compliance portal.

upvoted 1 times

Eltooth 2 months, 2 weeks ago

Selected Answer: A

A is correct answer: Yes

You must enable device monitoring and onboard your endpoints before you can monitor and protect sensitive items on a device. Both of these actions are done in the Microsoft Purview portal.

When you want to onboard devices that haven't been onboarded yet, you download the appropriate script and deploy it to those devices. Follow the device onboarding procedures below.

If you already have devices onboarded into Microsoft Defender for Endpoint, they'll already appear in the managed devices list.

https://learn.microsoft.com/en-us/purview/device-onboarding-overview#onboarding-windows-10-or-windows-11-devices

upvoted 1 times

a41c97a 2 months, 3 weeks ago

Selected Answer: A

To ensure that Microsoft 365 Endpoint Data Loss Prevention (Endpoint DLP) can protect content on Windows 11 devices, one of the mandatory prerequisites is to onboard the devices to Microsoft Defender for Endpoint.

upvoted 2 times

QuwQuw 2 months, 3 weeks ago

Selected Answer: A

Copilot: A

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 44 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 44

Topic #: 2

[All SC-401 Questions]

You are configuring a data loss prevention (DLP) policy to report when credit card data is found on a Microsoft Entra joined Windows device.

You plan to use information from the policy to restrict the ability to copy the sensitive data to the clipboard.

What should you configure in the policy advanced DLP rule?

A. user notifications

B. an action **Most Voted**

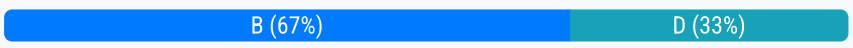
C. user overrides

D. the incident report

Hide Answer

Suggested Answer: *B*

Community vote distribution



by Seidor_Analytics at *Sept. 5, 2025, 8:15 a.m.*

Comments

Eltooth 2 months, 1 week ago

Selected Answer: B

Correct answer: B. an action
To restrict the ability to copy sensitive data (like credit card numbers) to the clipboard on a Microsoft Entra joined Windows device, you need to configure an action in the advanced DLP rule of your Endpoint DLP policy.
Explanation:
In Endpoint DLP, actions define what happens when sensitive data is detected. To block or audit clipboard activity, you configure:

Action: e.g., Audit, Block with override, or Block without override
Activity: e.g., Copy to clipboard, Print, Upload to cloud, etc.

Other options explained:

A. User notifications: Used to inform users when a policy is triggered, but doesn't enforce restrictions.
C. User overrides: Allows users to bypass a restriction with justification, but isn't the core setting to restrict clipboard use.
D. Incident report: Used for reporting and alerting, not for enforcing restrictions.

upvoted 2 times

RickySmith 3 months ago

Selected Answer: D

D is correct if you are configuring it only to report for now.
B is correct when you are configuring it to block.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 45 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 45

Topic #: 2

[All SC-401 Questions]

You plan to create a new data loss prevention (DLP) policy named DLP1.

DLP1 will be applied to the Exchange email location.

You need to exclude two users named User1 and User2 from DLP1.

What should you do first?

A. Create an organization sharing policy in Microsoft Exchange.

B. Create an advanced DLP rule.

C. Create a mail flow rule in Microsoft Exchange.

D. Create a distribution list that contains User1 and User2. **Most Voted**

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:17 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: D

D is correct answer: Create a DL that contains User1 and User2. (Edit Exchange scope from All groups --> Exclude groups --> exclude groups --> Add DL

upvoted 3 times

Caezarlay 2 months, 2 weeks ago

Selected Answer: D

Given answer is correct

upvoted 2 times

Gtc_ 3 months ago

Selected Answer: D

Add to Dist List then exclude mail from that list

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 46 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 46

Topic #: 2

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains three users named User, User2, and User3. The subscription contains the groups shown in the following table.

Name	Members
Group1	User1
Group2	User2, User3
Group3	User2, User2, User3

The subscription contains the devices shown in the following table.

Name	Platform
Device1	Windows
Device2	Android
Device3	macOS

All the devices are onboarded to Microsoft Purview.

You have the data loss prevention (DLP) policies shown in the following table.

Name	Assigned to	Description
Policy1	Group1	Restrict copying data to USB devices.
Policy2	Group2	Restrict copying data to a clipboard.
Policy3	Group3	Restrict accessing corporate content in Microsoft 365 locations.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
When User1 signs in to Device1, the user will be restricted from copying data to a USB storage device.	○	○
When User2 signs in to Device2, the user will be restricted from copying data to the clipboard.	○	○
When User3 signs in to Device3, the user will be restricted from accessing corporate content in Microsoft SharePoint Online.	○	○

Hide Answer

Suggested Answer:

Answer Area

Statements	Yes	No
When User1 signs in to Device1, the user will be restricted from copying data to a USB storage device.	◉	○
When User2 signs in to Device2, the user will be restricted from copying data to the clipboard.	○	◉
When User3 signs in to Device3, the user will be restricted from accessing corporate content in Microsoft SharePoint Online.	◉	○

by Seidor_Analytics at *Sept. 5, 2025, 8:17 a.m.*

Comments

Eltooth Highly Voted 2 months, 2 weeks ago

Yes - Windows 10/11 suported
No - Android not supported (MAM app protection should be used)
Yes - Supported (if OS is using three latest released versions)

https://learn.microsoft.com/en-gb/purview/dlp-learn-about-dlp#plan-for-dlp

upvoted 5 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 47 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 47

Topic #: 2

[All SC-401 Questions]

You create a retention label that has a retention period of seven years.

You need to ensure that documents containing a credit card number are retained for seven years. Other documents must not be retained.

What should you create?

A. a retention label policy of type auto-apply **Most Voted**

B. a retention label policy of type publish

C. a retention policy that deletes files automatically

D. a retention policy that retains files automatically

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:16 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: A

A is correct answer: a retention label of type auto-apply.

upvoted 3 times

Caezarlay 2 months, 2 weeks ago

Selected Answer: A

Given answer is correct

upvoted 2 times

Gtc_ 3 months ago

Selected Answer: A

Correct

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 48 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 48

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription.

A security manager receives an email message every time a data loss prevention (DLP) policy match occurs.

You need to limit alert notifications to actionable DLP events.

What should you do?

A. From the Microsoft Purview portal, modify the Policy Tips settings of a DLP policy.

B. From the Microsoft Defender portal, apply a filter to the alerts.

C. From the Microsoft Purview portal, modify the matched activities threshold of an alert policy. **Most Voted**

D. From the Microsoft Purview portal, modify the User overrides settings of a DLP policy.

Hide Answer

Suggested Answer: *C*

Community vote distribution

C (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:16 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: C

C. From the Microsoft Purview portal, modify the matched activities threshold of an alert policy.

upvoted 2 times

Caezarlay 2 months, 2 weeks ago

Selected Answer: C

Given answer is correct

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 49 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 49

Topic #: 2

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of security group
User1	Group1, Group2
User2	Group2
User3	Group1, Group3

You have the data loss prevention (DLP) policies shown in the following table.

Name	Location	Included	Number of DLP rules	Rule severity
DLP1	Devices	Group1	1	High
DLP2	Devices	Group2	1	Medium
DLP3	Devices	Group3	1	Medium

From Insider risk management, you configure a priority user group named PriGroup1 that contains User3 as a member.

You have the insider risk policies shown in the following table.

Name	Policy template	Trigger	Group
Policy1	Data leaks	DLP1	Group1
Policy2	Data leaks	DLP2	Group2
Policy3	Data leaks by priority users	DLP3	PriGroup1

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
When User3 performs an action that matches the rule for DLP1, Policy1 generates an alert.	○	○
When User1 performs an action that matches the rule for DLP2, Policy2 generates an alert.	○	○
When User3 performs an action that matches the rule for DLP3, Policy3 generates an alert.	○	○

Hide Answer

Suggested Answer:

Answer Area

Statements	Yes	No
When User3 performs an action that matches the rule for DLP1, Policy1 generates an alert.	◉	○
When User1 performs an action that matches the rule for DLP2, Policy2 generates an alert.	○	◉
When User3 performs an action that matches the rule for DLP3, Policy3 generates an alert.	◉	○

by Seidor_Analytics at *Sept. 5, 2025, 8:25 a.m.*

Comments

Eltooth 2 months ago

No
No
Yes

Policy1 will not generate an alert when User3 performs an action that matches the rule for DLP1.
DLP1 applies to Group1.
Policy1 is triggered by DLP1 and applies to Group1.
User3 is a member of Group1, so DLP1 can detect their activity.
However:
Policy1 is not scoped to PriGroup1, and it is not a priority user policy.
Insider risk policies only generate alerts for users in the policy's target group.
User3 is part of PriGroup1, but Policy1 does not include PriGroup1 — it includes Group1.

Even though User3 is in Group1, insider risk policies that are not scoped to priority users will not generate alerts for priority user activity unless explicitly configured to do so.

upvoted 1 times

Eltooth 2 months ago

DLP2 applies to Group2.
Policy2 is triggered by DLP2 and applies to Group2.
User3 is not a member of Group2 — User3 is in Group1 and Group3.

Summary:

User3 does not match DLP2 ❌
Policy2 is triggered by DLP2 ✅
Policy2 applies to Group2
User3 is not in Group2 ❌

Therefore, Policy2 will not generate an alert for User3's activity, because the user is not in the scope of the DLP policy or the insider risk policy.

upvoted 1 times

Eltooth 2 months ago

User3 is a member of Group3.
DLP3 applies to Group3, so User3's activity can trigger a match.
Policy3 is triggered by DLP3 and applies to PriGroup1.
User3 is also a member of PriGroup1, which is a priority user group configured in Insider Risk Management.

🔐 Insider Risk Policy Logic:

Policy3 uses the “Data leaks by priority users” template.
It is designed to monitor priority users (like User3) for risky behaviour.
Since User3 matches both the DLP3 rule and is in the target group of Policy3, the policy will generate an alert.

✅ Summary:
User3 matches DLP3
Policy3 is triggered by DLP3
Policy3 applies to PriGroup1
User3 is in PriGroup1

Therefore, Policy3 will generate an alert.

upvoted 1 times

Eltooth 2 months ago

CORRECTION:
User1 is a member of Group2.
DLP2 applies to Group2, so User1’s activity can trigger a match.
Policy2 is triggered by DLP2 and also applies to Group2.
Therefore, when User1 performs an action that matches the rule in DLP2, Policy2 is correctly scoped to generate an alert.

Summary:

User1 matches DLP2
Policy2 is triggered by DLP2
Policy2 applies to Group2
User1 is in Group2 ✅

Therefore, Policy2 will generate an alert.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 50 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 50

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2. The subscription has a data loss prevention (DLP) policy named Policy1.

User2 sends an outbound message that generates a false positive for Policy1.

You need to ensure that User1 can download the message that generated the alert. The solution must follow the principle of least privilege.

To which role group should you add User1?

A. Data Investigator **Most Voted**

B. Security Operator

C. eDiscovery Manager

D. Global Reader

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:16 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: A

A is correct answer: Data investigator
Security Operator cannot Export
eDiscovery Manager is too powerful
Global Reader cannot export.

https://learn.microsoft.com/en-us/defender-office-365/scc-permissions

upvoted 2 times

florinvele 2 months, 4 weeks ago

Selected Answer: A

Data Investigator role group has the Export role which allows to download message returned by content search

upvoted 3 times

Gtc_ 3 months ago

Selected Answer: A

Global reader can’t download the original message

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 51 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 51

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that contains the adaptive scopes shown in the following table.

Name	Type	Query
Scope1	Users	`FirstName starts with User`
Scope2	SharePoint Online sites	`SiteTitle starts with Site`

You create the retention policies shown in the following table.

Name	Type	Location
RPolicy1	Adaptive	Scope1
RPolicy2	Adaptive	Scope2
RPolicy3	Static	Microsoft 365 groups

Which retention policies support a preservation lock?

A. RPolicy2 only

B. RPolicy3 only **Most Voted**

C. RPolicy1 and RPolicy2 only

D. RPolicy1 and RPolicy3 only

E. RPolicy1, RPolicy2, and RPolicy3

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:15 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: B

B is correct answer: RPolicy 3 only

"Currently, adaptive policy scopes don't support Preservation Lock."
https://learn.microsoft.com/en-us/purview/retention-preservation-lock

upvoted 2 times

RickySmith 2 months, 2 weeks ago

Selected Answer: B

https://learn.microsoft.com/en-us/purview/retention-preservation-lock
Currently, adaptive policy scopes don't support Preservation Lock.

upvoted 3 times

Gtc_ 3 months ago

Selected Answer: B

Adaptive doesn’t support locks currently

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 52 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 52

Topic #: 2

[All SC-401 Questions]

You need to provide a user with the ability to view data loss prevention (DLP) alerts in the Microsoft Purview portal. The solution must use the principle of least privilege.

Which role should you assign to the user?

A. Security Operator

B. Security Reader **Most Voted**

C. Compliance Data Administrator

D. Compliance Administrator

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:24 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: B

B is correct answer: Security Reader

https://learn.microsoft.com/en-us/defender-office-365/scc-permissions

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 53 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 53

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription. The subscription contains 500 Windows devices that are onboarded to Microsoft Purview.

You need to prevent users from sharing sensitive information with third-party generative AI websites.

Which Microsoft Purview solution should you use?

A. Data Loss Prevention **Most Voted**

B. Insider Risk Management

C. Information Protection

D. Information Barriers

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:18 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: A

A is correct answer.

DLP can be applied to "Data in browser and network activity" that can be scoped to OpenAI ChatGPT, Google Gemini, Copilot and DeekSeek.

Note: This requires a PAYG sub...

upvoted 2 times

Gtc_ 3 months ago

Selected Answer: A

Correct

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 54 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 54

Topic #: 2

[All SC-401 Questions]

You create a label that encrypts email data.

Users report that they cannot use the label in Outlook on the web to protect the email messages they send.

You need to ensure that the users can use the new label to protect their email.

What should you do?

A. Create a label policy. **Most Voted**

B. Wait six hours and ask the users to try again.

C. Create a new sensitive information type.

D. Modify the priority order of label policies.

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:16 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: A

A is correct answer. Create a label policy (to apply the label based on conditions and to scope)

upvoted 2 times

Gtc_ 3 months ago

Selected Answer: A

Label wont do anything without policy

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 55 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 55

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 subscription. You create a retention policy and apply the policy to Exchange Online mailboxes.

You need to ensure that the retention policy tags can be assigned to mailbox items as soon as possible.

What should you do?

A. From the Microsoft Purview portal, create a data loss prevention (DLP) policy.

B. From the Microsoft Purview portal, create a label policy.

C. From Exchange Online PowerShell, run Start-ManagedFolderAssistant. **Most Voted**

D. From Exchange Online PowerShell, run Start-RetentionAutoTagLearning.

Hide Answer

Suggested Answer: *C*

Community vote distribution

C (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:25 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: C

C is correct answer.

"The Managed Folder Assistant is a process that applies retention policy settings to mailboxes. In a normal cycle, the assistant processes mailboxes in Exchange Online once every seven days. Manually running the assistant immediately processes the specified mailbox, making the retention tags available right away."

https://learn.microsoft.com/en-us/powershell/module/exchangepowershell/start-managedfolderassistant?view=exchange-ps#description

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 56 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 56

Topic #: 2

[All SC-401 Questions]

You have Microsoft 365 E5 tenant that uses Microsoft Teams and contains two users named User1 and User2.

You create a data loss prevention (DLP) policy that is applied to the Teams chat and channel messages location for User1 and User2.

Which Teams entities will have DLP protection?

A. 1:1/n chats and general channels only

B. 1:1/n chats and private channels only

C. 1:1/n chats, general channels, and private channels **Most Voted**

Hide Answer

Suggested Answer: *C*

Community vote distribution

C (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:24 a.m.*

Comments

Gtc_ **Highly Voted** 3 months ago

Selected Answer: C

"DLP Licensing for Microsoft Teams
Data loss prevention capabilities include Microsoft Teams chat and channel messages, including private channel messages for:
Office 365 E5/A5/G5
Microsoft 365 E5/A5/G5
Microsoft 365 E5/A5/G5 Information Protection and Governance
Microsoft 365 E5/A5/G5/F5 Compliance and F5 Security & Compliance
Office 365 and Microsoft 365 E3 include DLP protection for SharePoint, OneDrive, and Exchange. This also includes files that are shared through Teams because Teams uses SharePoint and OneDrive to share files.
Support for DLP protection in Teams Chat requires an E5 license."

upvoted 7 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 57 DISCUSSION

Actual exam question from Microsoft's SC-401

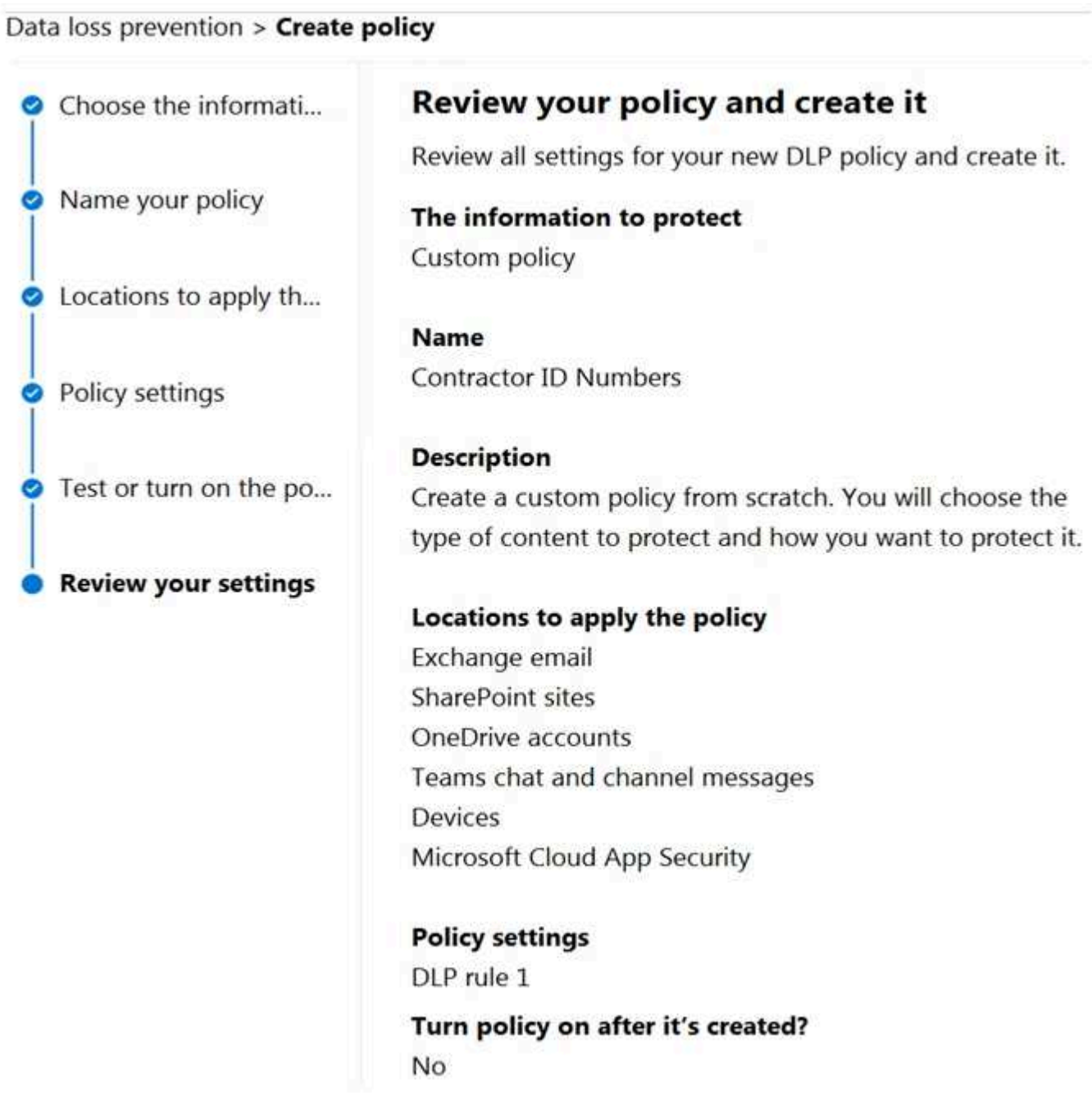
Question #: 57

Topic #: 2

[All SC-401 Questions]

You create a data loss prevention (DLP) policy. The Advanced DLP rules page is shown in the Rules exhibit. (Click the Rules tab)

The Review your settings page is shown in the Review exhibit. (Click the Review tab.)


Data loss prevention > Create policy
Choose the informati...
Name your policy
Locations to apply th...
Policy settings
Test or turn on the po...
Review your settings
Review your policy and create it
Review all settings for your new DLP policy and create it.
The information to protect
Custom policy
Name
Contractor ID Numbers
Description
Create a custom policy from scratch. You will choose the type of content to protect and how you want to protect it.
Locations to apply the policy
Exchange email
SharePoint sites
OneDrive accounts
Teams chat and channel messages
Devices
Microsoft Cloud App Security
Policy settings
DLP rule 1
Turn policy on after it's created?
No

You need to review the potential impact of enabling the policy without applying the actions.

What should you do?

A. Exit the policy, and then select I'd like to test it out first. **Most Voted**

B. Edit the policy, remove all the actions in DLP rule 1, and select I'd like to test it out first.

C. Edit the policy, remove the Restrict access to the content and Send incident report to Administrator actions, and then select Yes, turn it on right away.

D. Edit the policy, remove all the actions in DLP rule 1, and select Yes, turn it on right away.

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:16 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: A

A is correct answer. Test policy after creating it.

upvoted 2 times

Gtc_ 3 months ago

Selected Answer: A

Correct answer

upvoted 3 times

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 58 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 58
Topic #: 2
[All SC-401 Questions]

You have a Microsoft 365 E5 tenant.

You create a data loss prevention (DLP) policy.

You need to ensure that the policy protects documents in Microsoft Teams chat sessions.

Which location should you enable in the policy?

A. SharePoint sites

B. Teams chat and channel messages

C. Exchange email

D. OneDrive accounts **Most Voted**

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (82%) B (18%)

by Seidor_Analytics at *Sept. 5, 2025, 8:24 a.m.*

Comments

337257e **Highly Voted** 2 months, 3 weeks ago

Selected Answer: D

seidor is garbage

upvoted 9 times

Eltooth **Most Recent** 2 months, 1 week ago

Selected Answer: B

Correct answer: B. Teams chat and channel messages
Explanation:
To ensure that a Data Loss Prevention (DLP) policy protects documents shared in Microsoft Teams chat sessions, you must enable the

Teams chat and channel messages location in the policy.
This location allows DLP to inspect and take action on:

1:1 and group chat messages
Messages in standard and private channels
Attachments shared in chats and channels

Why the other options are incorrect:

A. SharePoint sites: Protects documents stored in SharePoint, not Teams chat messages.
C. Exchange email: Applies to email messages, not Teams.
D. OneDrive accounts: Applies to files stored in OneDrive, not Teams chat content.

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 59 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 59

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription.

You create a data loss prevention (DLP) policy and select Use Notifications to inform your users and help educate them on the proper use of sensitive info.

Which apps will show the policy tip?

A. Outlook on the web only

B. Outlook Win32 only

C. Outlook for iOS and Android only

D. Outlook on the web and Outlook Win32 only **Most Voted**

E. Outlook Win32 and Outlook for iOS and Android only

F. Outlook on the web, Outlook Win32, and Outlook for iOS and Android

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (73%) F (27%)

by Seidor_Analytics at *Sept. 5, 2025, 8:18 a.m.*

Comments

florinvele **Highly Voted** 2 months, 4 weeks ago

Selected Answer: D

Android does not support tips

upvoted 5 times

Eltooth **Most Recent** 2 months, 1 week ago

Selected Answer: D

As of mid-August 2025, Outlook for iOS and Android officially supports Microsoft Purview DLP policy tips and enforcement, aligning with the desktop and web versions.
What this means:

Users on mobile devices will now receive inline alerts or pop-ups when attempting to send messages containing sensitive information (e.g., credit card numbers, national IDs).
These alerts are based on admin-configured DLP rules.
The feature is enabled by default and requires no additional configuration or licensing if DLP is already in use for Outlook desktop or web.

Important Note:
Although this feature was initially rolled out, Microsoft temporarily rolled it back in late September 2025 for further review. Organizations should monitor the Microsoft 365 Message Center for updates on its re-release.

upvoted 3 times

Dicornyt 3 months ago

Selected Answer: F

https://learn.microsoft.com/en-us/purview/dlp-policy-tips-reference

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 60 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 60

Topic #: 2

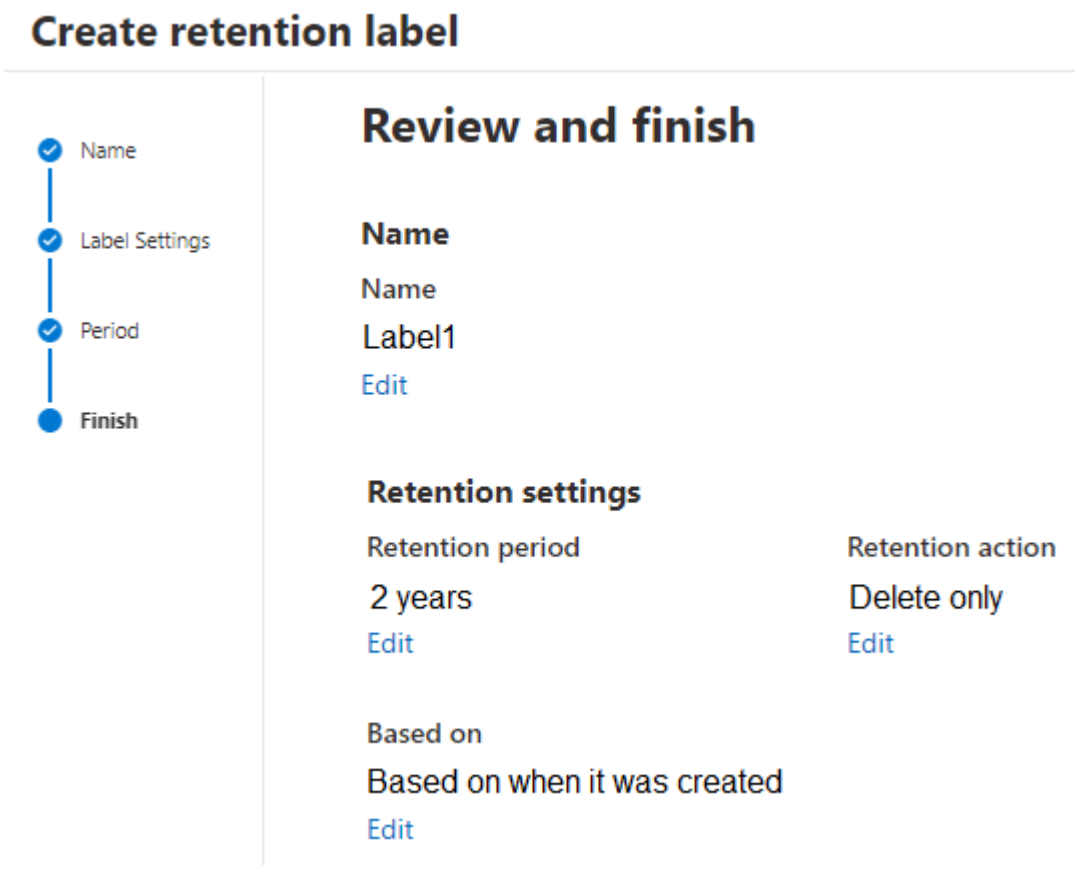
[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 subscription.

You create a retention label named Label1 as shown in the following exhibit.



You publish Label1 to SharePoint sites.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

If you create a file in a Microsoft SharePoint library on January 1, 2025, and apply Label1 to the file, you can

- never delete the file
- delete the file before January 1, 2025
- delete the file after January 1, 2025

If you create a file in a Microsoft SharePoint library on March 15, 2025, and apply Label1 to the file, the file will

- always remain in the library
- remain in the library until you delete the file
- be deleted automatically on March 15, 2027

Hide Answer

Suggested Answer:

Answer Area

If you create a file in a Microsoft SharePoint library on January 1, 2025, and apply Label1 to the file, you can

- never delete the file
- delete the file before January 1, 2025
- delete the file after January 1, 2025

If you create a file in a Microsoft SharePoint library on March 15, 2025, and apply Label1 to the file, the file will

- always remain in the library
- remain in the library until you delete the file
- be deleted automatically on March 15, 2027

by Seidor_Analytics at *Sept. 5, 2025, 8:25 a.m.*

Comments

RickySmith 3 months ago

3 - You can definitely delete the file, but only after it is created.
3 - Policy

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 61 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 61

Topic #: 2

[All SC-401 Questions]

SIMULATION

-

Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and select the username below.

To enter your password, place your cursor in the Enter password box and select the password below.

Microsoft 365 Username:
admin@WWLx971455.onmicrosoft.com

Microsoft 365 Password: XXXXXXXXX

If the Microsoft Edge browser or Microsoft 365 portal does not load successfully, select the Microsoft Edge browser icon from the task bar, type the URL “https://admin microsoft.com”, and press Enter.

The following information is for technical support purposes only:
Lab Instance: XXXXXXXX.

Task 4

-

You need to block users from sending emails containing information that is subject to Payment Card Industry Data Security Standard (PCI DSS). The solution must affect only emails.

Hide Answer

Suggested Answer:

Note: Policy templates
DLP policy templates are sorted into four categories:

* policies that can detect and protect types of Financial information.
Includes PCI Data Security Standard (PCI DSS), Credit card number
* Medical and health
* Privacy
* Custom policy

Use the EAC to configure a DLP policy from a template
Step 1: In the EAC, navigate to Compliance management > Data loss prevention, and then click Add Add Icon.

Step 2: On the Create a new DLP policy from a template page, complete the following fields:

Step 3: Name: Add a name that will distinguish this policy from others.

Step 4: Description: Add an optional description that summarizes this policy.

Step 5: Choose a template: Select the appropriate template to begin creating a new policy.

Step 6: Select the Payment Card Industry Data Security Standard (PCI DSS) template.

Step 7: More options: Select the mode or state. The new policy is not fully enabled until you specify that it should be. The default mode for a policy is test without notifications.

Step 8: Click Save to finish creating the policy.

Reference:
https://learn.microsoft.com/en-us/purview/dlp-policy-reference
https://learn.microsoft.com/en-us/exchange/security-and-compliance/data-loss-prevention/create-dlp-policy-from-template

by Seidor_Analytics at *Sept. 5, 2025, 8:18 a.m.*

Comments

Eltooth 2 months, 1 week ago
Financial --> PCI DSS template policy
upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 62 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 62

Topic #: 2

[All SC-401 Questions]

SIMULATION

-

Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and select the username below.

To enter your password, place your cursor in the Enter password box and select the password below.

Microsoft 365 Username:
admin@WWLx971455.onmicrosoft.com

Microsoft 365 Password: XXXXXXXXX

If the Microsoft Edge browser or Microsoft 365 portal does not load successfully, select the Microsoft Edge browser icon from the task bar, type the URL “https://admin microsoft.com”, and press Enter.

The following information is for technical support purposes only:
Lab Instance: XXXXXXXX.

Task 5

-

You need to ensure that a group named U.S. Sales can store files containing information subject to General Data Protection Regulation (GDPR) in their OneDrive accounts. All other current GDPR restrictions must remain in effect.

Hide Answer

Suggested Answer:

Note: Policy templates
DLP policy templates are sorted into four categories:

* policies that can detect and protect types of Financial information.
* Medical and health
* Privacy
- Includes General Data Protection Regulation (GDPR) Enhanced
* Custom policy

Step 1: Sign in to the Microsoft Purview compliance portal.

Step 2: In the Microsoft Purview compliance portal > left navigation > Solutions > Data loss prevention > Policies > + Create policy.

Step 3: Select Custom from the Categories list.

Step 4: Select Custom from the Regulations list.

Step 5: Give the policy a name.

Step 6: Fill in a description. (Skip)

Step 7: Select Next.

Step 8: Select Full directory under Admin units.

Step 9: Set the OneDrive location status to On. Set all the other location status to Off.

Step 10: Edit the OneDrive accounts scope. Select All users and group >Include users and groups > + Include > Include groups and add the U.S. Sales group.

Question is: You need to ensure that a group named U.S. Sales can store files containing information subject to General Data Protection Regulation (GDPR) in their OneDrive accounts. All other current GDPR restrictions must remain in effect.

Step 11: Select Done. Select Done. Select Next.

Step 12: On the Define policy settings page, the Create or customize advanced DLP rules option should already be selected.

Step 13: Select Next. Select Create rule. Name the rule and provide a description.

Step 14: Under Conditions select + Add condition >

Step 15: Select Content contains > Add > Sensitive info types > General Data Protection Regulation (GDPR). Choose Add.
Step 16: Under Actions, select Add an action > Allow Access (or similar)

Step 17: Finish the wizard: Choose Save. Choose Next. Choose Done

Reference:
https://learn.microsoft.com/en-us/purview/dlp-policy-reference
https://learn.microsoft.com/en-us/purview/dlp-create-deploy-policy

by Seidor_Analytics at *Sept. 5, 2025, 8:24 a.m.*

Comments

bobg 2 weeks, 4 days ago

I'm guessing there is an existing policy there that sales needs to be added as an exclusion to

upvoted 1 times

Eltooth 2 months, 1 week ago

No need for a custom policy - Use Privacy --> GDPR Enhanced template.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 65 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 65

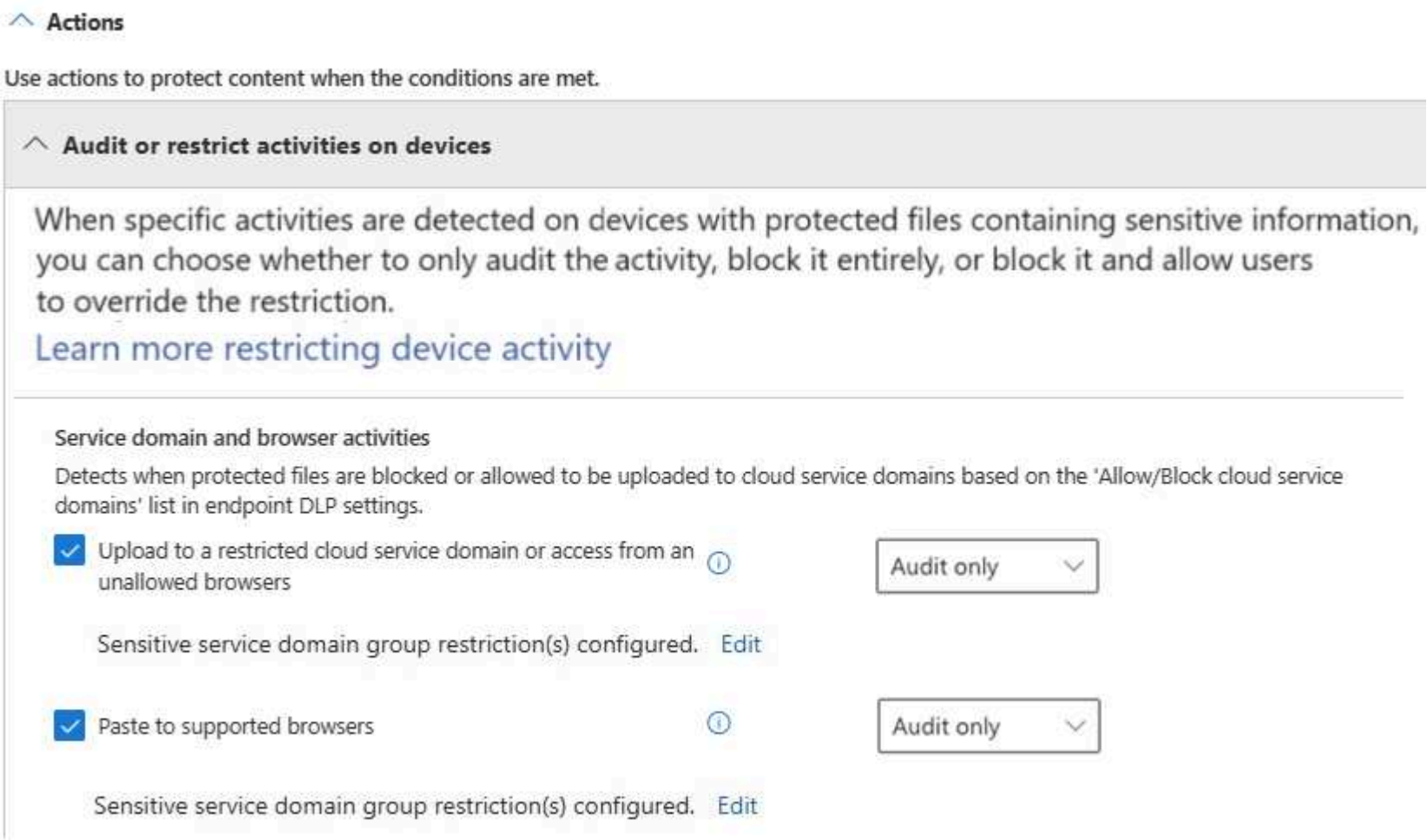
Topic #: 2

[All SC-401 Questions]

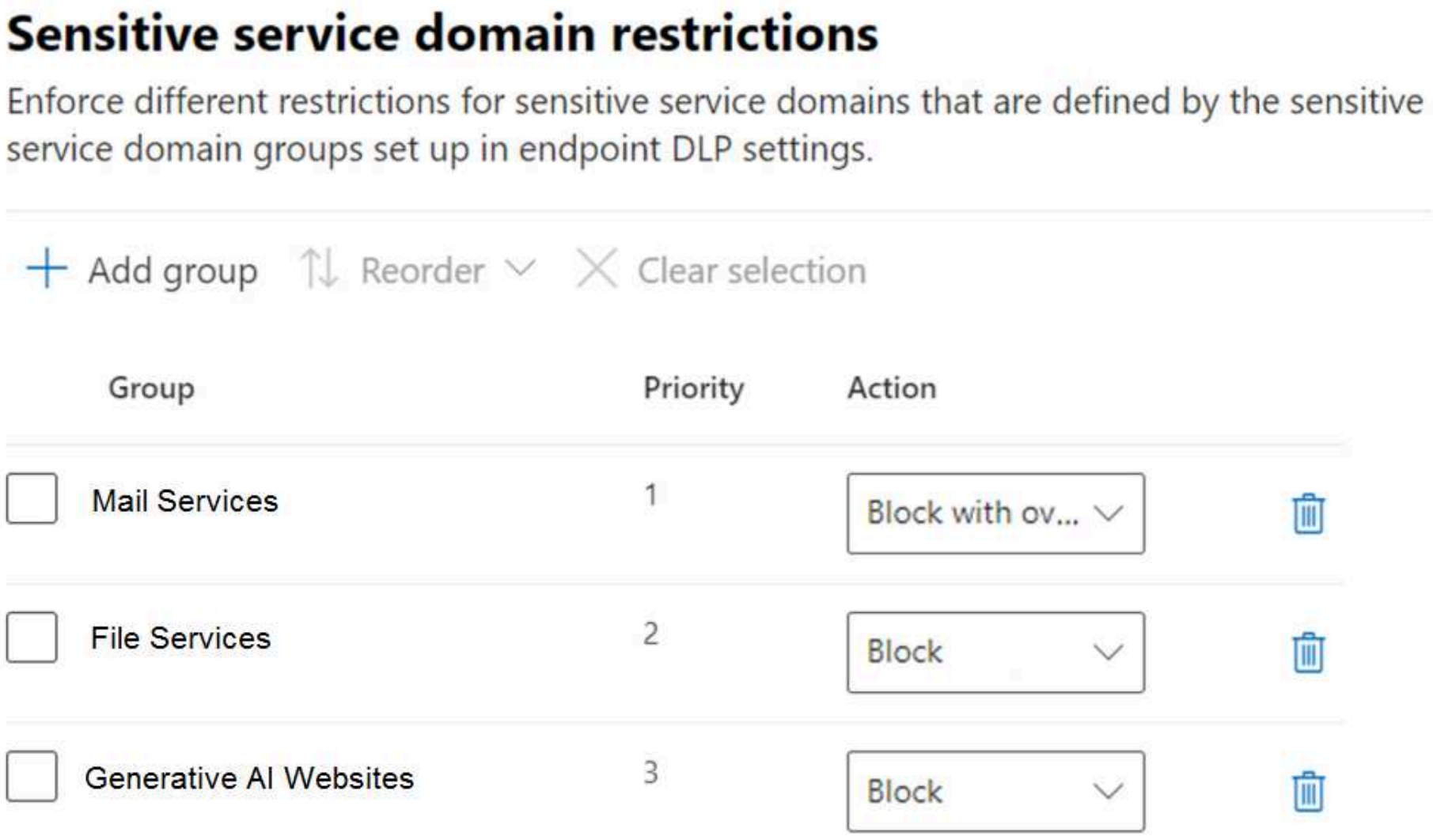
HOTSPOT

-

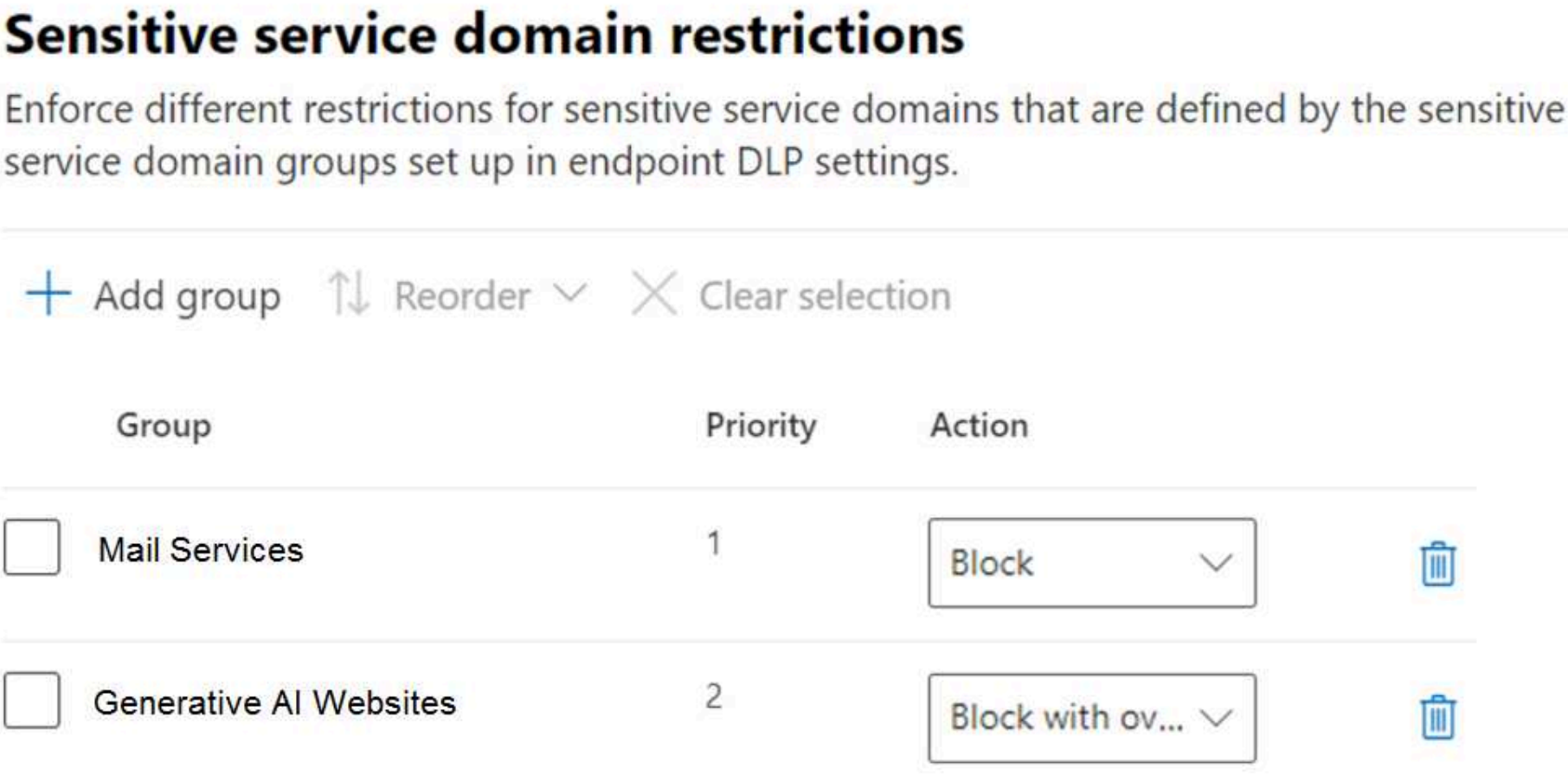
You have a Microsoft 365 ES subscription that contains a user named User1. The subscription contains an Endpoint data loss prevention (Endpoint DLP) policy as shown in the Actions exhibit. (Click the Actions tab.)


Actions
Use actions to protect content when the conditions are met.
Audit or restrict activities on devices
When specific activities are detected on devices with protected files containing sensitive information, you can choose whether to only audit the activity, block it entirely, or block it and allow users to override the restriction.
Learn more restricting device activity
Service domain and browser activities
Detects when protected files are blocked or allowed to be uploaded to cloud service domains based on the 'Allow/Block cloud service domains' list in endpoint DLP settings.
Upload to a restricted cloud service domain or access from an unallowed browsers
Audit only
Sensitive service domain group restriction(s) configured. Edit
Paste to supported browsers
Audit only
Sensitive service domain group restriction(s) configured. Edit

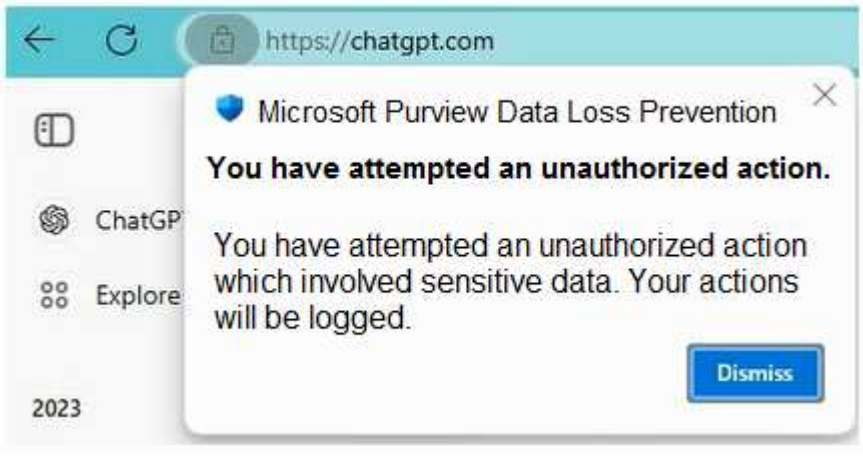
You configure the Upload to a restricted cloud service domain or access from an unallowed browsers settings as shown in the Upload restrictions exhibit. (Click the Upload restrictions tab.)



You configure the Paste to supported browsers settings as shown in the Paste restrictions exhibit. (Click the Paste restrictions tab.)



When User1 pastes content into ChatGPT, the user receives the error message shown in the Error exhibit. (Click the Error tab.)



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can paste sensitive data from an email to ChatGPT after selecting **Dismiss**.	○	○
User1 can upload emails that contain sensitive data to ChatGPT after selecting **Dismiss**.	○	○
User1 can paste sensitive data from a Microsoft Word document to ChatGPT after selecting **Dismiss**.	○	○

Hide Answer

Suggested Answer:

Answer Area

Statements	Yes	No
User1 can paste sensitive data from an email to ChatGPT after selecting **Dismiss**.	◉	○
User1 can upload emails that contain sensitive data to ChatGPT after selecting **Dismiss**.	○	◉
User1 can paste sensitive data from a Microsoft Word document to ChatGPT after selecting **Dismiss**.	◉	○

by Seidor_Analytics at *Sept. 5, 2025, 8:18 a.m.*

Comments

Alcpt 2 weeks, 2 days ago

i think the given answer is correct. 1 and 3 allow override.

upvoted 1 times

Eltooth 2 months ago

No
No
No

User1 can paste sensitive data from an email to ChatGPT after selecting Dismiss → No (Dismiss only closes the message; the paste remains blocked.)

User1 can upload emails that contain sensitive data to ChatGPT after selecting Dismiss → No (Uploads to Generative AI Websites are fully blocked.)

User1 can paste sensitive data from a Microsoft Word document to ChatGPT after selecting Dismiss → No (Same reason as #1; paste is blocked.)

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 66 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 66

Topic #: 2

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 E5 subscription that uses Microsoft Purview and just-in-time (JIT) protection. Fallback action in case of failure is set to Block users from completing actions.

The subscription contains the users shown in the following table.

Name	JIT protection scope
User1	Included
User2	Not configured
User3	Included

The subscription contains the devices shown in the following table.

Name	Microsoft Defender
Device1	Onboarded
Device2	Onboarded
Device3	Not onboarded

The devices contain the files shown in the following table.

Name	File classification evaluation status	Location
File1.docx	Not evaluated	Device1
File2.pdf	Evaluated	Device2
File3.xlsx	Not evaluated	Device3

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If User1 attempts to copy File1.docx to a removable USB drive, JIT will block the action.	○	○
If User2 signs in to Device2 and attempts to attach File2.pdf to an email, JIT will block the action.	○	○
If User3 attempts to copy File3.xlsx to a network share, JIT will generate an audit event.	○	○

Hide Answer

Suggested Answer:

Answer Area

Statements	Yes	No
If User1 attempts to copy File1.docx to a removable USB drive, JIT will block the action.	☑	○
If User2 signs in to Device2 and attempts to attach File2.pdf to an email, JIT will block the action.	○	☑
If User3 attempts to copy File3.xlsx to a network share, JIT will generate an audit event.	○	☑

by Seidor_Analytics at *Sept. 5, 2025, 8:25 a.m.*

Comments

RickySmith Highly Voted 2 months, 2 weeks ago

Y - User/Device onboarded and protected and fallback set to block, so "Not evaluated" file will be blocked.
N - User 2 is not included in scope for JIT protection
N - Device is not onboarded to Defender

upvoted 5 times

Farreller Most Recent 2 weeks, 4 days ago

If User1 attempts to copy File1.docx to a removable USB drive, JIT will block the action.

User1 is in JIT scope ✅
Device1 is onboarded
File1.docx is not evaluated ❌
→ JIT cannot enforce without classification.
Answer: No

If User2 signs in to Device2 and attempts to attach File2.pdf to an email, JIT will block the action.

User2 is not configured for JIT
Even though Device2 is onboarded and File2.pdf is evaluated, JIT does not apply to User2.
Answer: No

If User3 attempts to copy File3.xlsx to a network share, JIT will generate an audit event.

User3 is in JIT scope ✅
Device3 is not onboarded
File3.xlsx is not evaluated
→ No enforcement or audit because device is not onboarded.
Answer: No

✅ Final Answers:

Statement 1: No

Statement 2: No
Statement 3: No

upvoted 2 times

Alcpt 2 weeks, 2 days ago

Yes , No, No
File1.docx (Not evaluated) - JIT can still protect it based on location/user policies. JIT primarily needs device onboarding and user scope - file classification enhances precision but isn't required for basic JIT functionality.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 67 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 67

Topic #: 2

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 E5 subscription.

You need to implement Endpoint data loss prevention (Endpoint DLP) to meet the following requirements:

- Ensure that users can upload data to only two sites named Site1 and Site2.
- Prevent users from pasting data to two search engines named Search1 and Search2.
- Minimize the number of policies and groups.

What is the minimum number of sensitive service domain groups and Endpoint DLP policies required? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

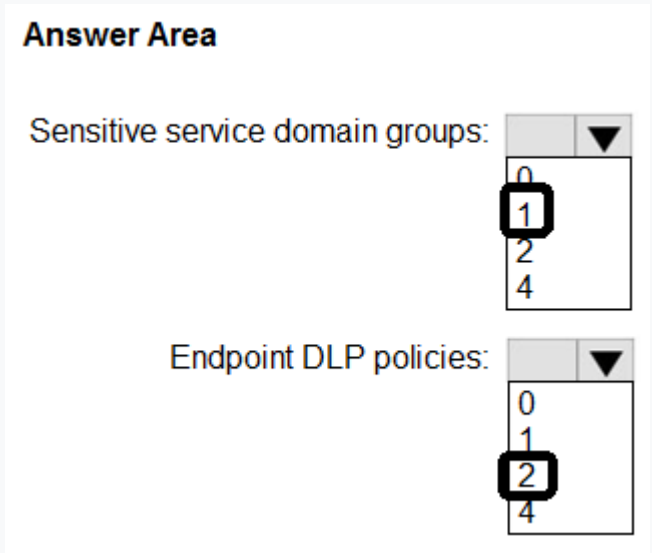
Answer Area

Sensitive service domain groups: 0 1 2 4

Endpoint DLP policies: 0 1 2 4

Hide Answer

Suggested Answer:



by Seidor_Analytics at *Sept. 5, 2025, 8:18 a.m.*

Comments

Caezarlay Highly Voted 2 months, 2 weeks ago

I will go with
Sensitive service domain groups: 2
Endpoint DLP policies: 1

upvoted 9 times

Eltooth Most Recent 2 months ago

2 & 2
Go to Microsoft Purview → Data Loss Prevention → Endpoint DLP settings.
Under Sensitive service domain groups, click Add group.
Group 1: Name it Allowed Upload Sites, add Site1.com and Site2.com.
Group 2: Name it Blocked Paste Sites, add Search1.com and Search2.com.

Step 2: Create Endpoint DLP Policy for Uploads
Navigate to Data Loss Prevention → Policies → Create policy.
Choose Custom policy → Endpoint DLP.
Configure: Locations: Devices.
Actions: Upload to restricted domains → Block.
Add exception for Group 1 (Allowed Upload Sites) → Allow.
Set mode to Enforce.

Step 3: Create Endpoint DLP Policy for Paste
Create another Endpoint DLP policy.
Configure: Locations: Devices.
Actions:Paste to supported browsers → Block for Group 2 (Blocked Paste Sites).
Set mode to Enforce.

upvoted 1 times

Eltooth 2 months ago

✅ Result:
Users can upload only to Site1 and Site2.
Users cannot paste into Search1 or Search2.
Only 2 groups and 2 policies used (minimum possible).

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 68 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 68

Topic #: 2

[All SC-401 Questions]

DRAG DROP

-

You have a Microsoft 365 E5 subscription.

You need to prevent the sharing of sensitive information in Microsoft Teams.

Which entities can you protect by applying a data loss prevention (DLP) policy to each resource?

To answer, drag the appropriate activities to the correct entity. Each activity may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Activities

- 1:1/n chats only
- Private channels only
- General chats only
- 1:1/n chats and private channels only
- 1:1/n chats and general chats only
- Private channels and general chats only
- 1:1/n chats, private channels, and general

Answer Area

User accounts:	
Microsoft 365 groups:	
Security groups or distribution lists:	

Hide Answer

Suggested Answer:

by Seidor_Analytics at *Sept. 5, 2025, 8:16 a.m.*

Comments

9ebaad0 3 weeks, 5 days ago

They have since updated the MS Learn page Eltooth & Dicornyt refer to as of October 30th the site now reads:
User Accounts: 1:1 Chats only
Security & Distribution Groups: 1:1 Chats only
M365 Groups: 1:1 chats, general channel messages & private channel messages.
Checked on the wayback machine that it did previously say their answers before 10/30.

upvoted 2 times

Eltooth 2 months, 1 week ago

User accounts: 1:1/n chats and private channels only
Microsoft 365 groups: 1:1/n chats and general chats only
Security groups or distribution lists: 1:1/n chats and private channels only

https://learn.microsoft.com/en-us/purview/dlp-microsoft-teams#scope-of-dlp-protection

upvoted 2 times

Caezarlay 2 months, 2 weeks ago

User accounts: Can protect 1:1/n chats and private channels, but not standard/shared channels.

Microsoft 365 groups: Can protect all Teams modalities—1:1/n chats, standard/shared channels, and private channels.

Security groups: Behave similarly to user accounts in DLP scope—no protection for standard/shared channels, but coverage for 1:1/n chats and private channels.

upvoted 1 times

Dicornyt 3 months ago

User accounts: 1:1/n chats and private channels only
Microsoft 365 groups: 1:1/n chats and general chats only
Security groups or distribution lists: 1:1/n chats and private channels only

https://learn.microsoft.com/en-us/purview/dlp-microsoft-teams

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 69 DISCUSSION

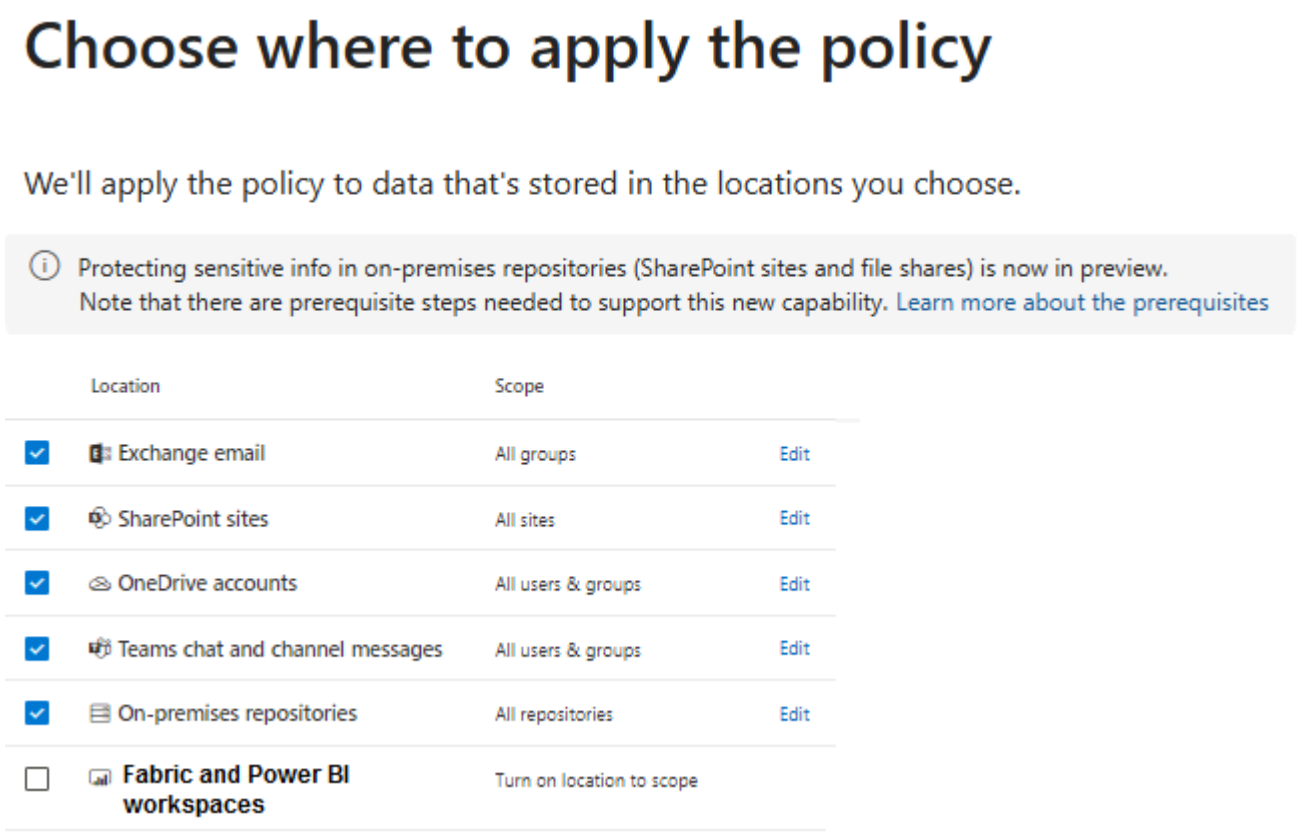
Actual exam question from Microsoft's SC-401

Question #: 69

Topic #: 2

[All SC-401 Questions]

You are creating a DLP policy named Policy1 that will be applied to the locations as shown in the following exhibit.


Choose where to apply the policy
We'll apply the policy to data that's stored in the locations you choose.
Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview.
Note that there are prerequisite steps needed to support this new capability. Learn more about the prerequisites
Location
Scope
Exchange email
All groups
Edit
SharePoint sites
All sites
Edit
OneDrive accounts
All users & groups
Edit
Teams chat and channel messages
All users & groups
Edit
On-premises repositories
All repositories
Edit
Fabric and Power BI workspaces
Turn on location to scope

Policy1 contains an advanced data loss prevention (DLP) rule named Rule1.

Which two conditions can you use in Rule1? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Document property is

B. Attachment's file extension is

C. Document size equals or is greater than

D. Content is shared from Microsoft 365 **Most Voted**

E. Content contains **Most Voted**

Hide Answer

Suggested Answer: *DE*

Community vote distribution

DE (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:24 a.m.*

Comments

Eltooth 2 months, 1 week ago

Selected Answer: DE

D and E are correct answers.

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 70 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 70
Topic #: 2
[All SC-401 Questions]

You have a data loss prevention (DLP) policy that applies to the Devices location. The policy protects documents that contain United States passport numbers.

Users report that they cannot upload documents to a travel management website because of the policy.

You need to ensure that the users can upload the documents to the travel management website. The solution must prevent the protected content from being uploaded to other locations.

Which Microsoft 365 Endpoint data loss prevention (Endpoint DLP) setting should you configure?

A. Service domains **Most Voted**

B. Unallowed apps

C. Unallowed browsers

D. File path exclusions

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:25 a.m.*

Comments

Eltooth 2 months, 1 week ago

Selected Answer: A

A is correct answer: Service Domains

upvoted 2 times

RickySmith 2 months, 2 weeks ago

Selected Answer: A

Service Domains will allow you to configure the sites to allow to while leaving it blocked for the others.

upvoted 2 times

Caezarlay 2 months, 2 weeks ago

Selected Answer: A

Given answer is correct

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 72 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 72

Topic #: 2

[All SC-401 Questions]

You need to create a retention policy to delete content after seven years from the following locations:

- Exchange Online email
- SharePoint Online sites
- OneDrive accounts
- Microsoft 365 Groups
- Teams channel messages
- Teams chats

What is the minimum number of retention policies that you should create?

A. 1

B. 2 **Most Voted**

C. 3

D. 4

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:24 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: B

B is correct answer : 2

One for teams channel & chats
One for the rest listed

Note : AI or copilot require individual policies as well.

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 72 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 72

Topic #: 2

[All SC-401 Questions]

You need to create a retention policy to delete content after seven years from the following locations:

- Exchange Online email
- SharePoint Online sites
- OneDrive accounts
- Microsoft 365 Groups
- Teams channel messages
- Teams chats

What is the minimum number of retention policies that you should create?

A. 1

B. 2 **Most Voted**

C. 3

D. 4

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:24 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: B

B is correct answer : 2

One for teams channel & chats
One for the rest listed

Note : AI or copilot require individual policies as well.

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 73 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 73

Topic #: 2

[All SC-401 Questions]

HOTSPOT

-

You create a retention label policy named Contoso Policy that contains the following labels:

10 years then delete

5 years then delete

Do not retain

-

Contoso_Policy is applied to content in Microsoft SharePoint Online sites.

After a couple of days, you discover the following messages on the Properties page of the label policy:

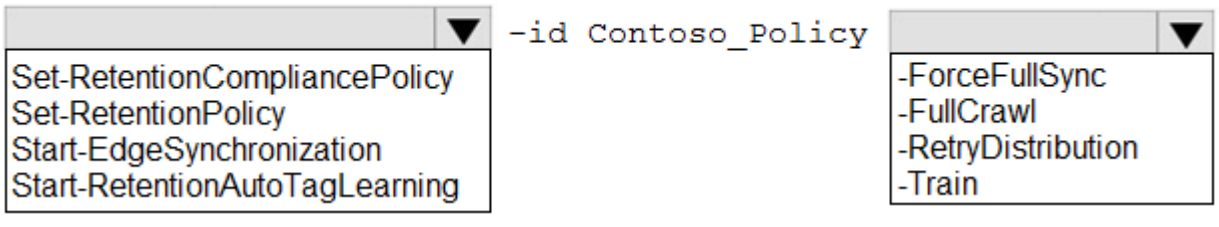
- Status: Off (Error)
- It's taking longer than expected to deploy the policy

You need to reinitiate the policy.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

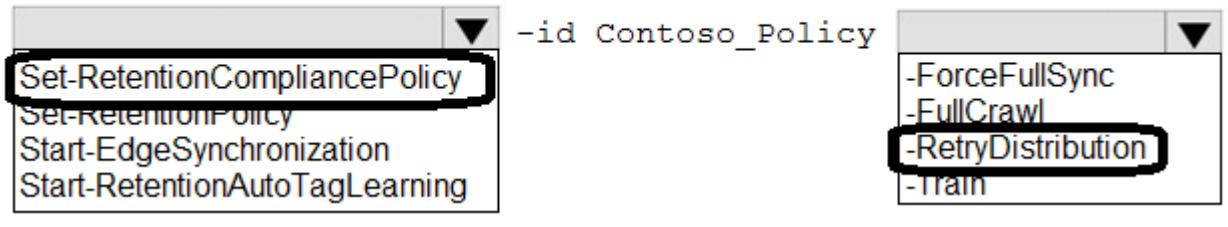
Answer Area



Hide Answer

Answer Area

Suggested Answer:



by Seidor_Analytics at *Sept. 5, 2025, 8:17 a.m.*

Comments

Eltooth 2 months, 1 week ago

Set-RetentionCompliancePolicy -id Contoso_Policy -RetryDistribution

https://learn.microsoft.com/en-us/powershell/module/exchangepowershell/set-retentioncompliancepolicy?view=exchange-ps

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 74 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 74

Topic #: 2

[All SC-401 Questions]

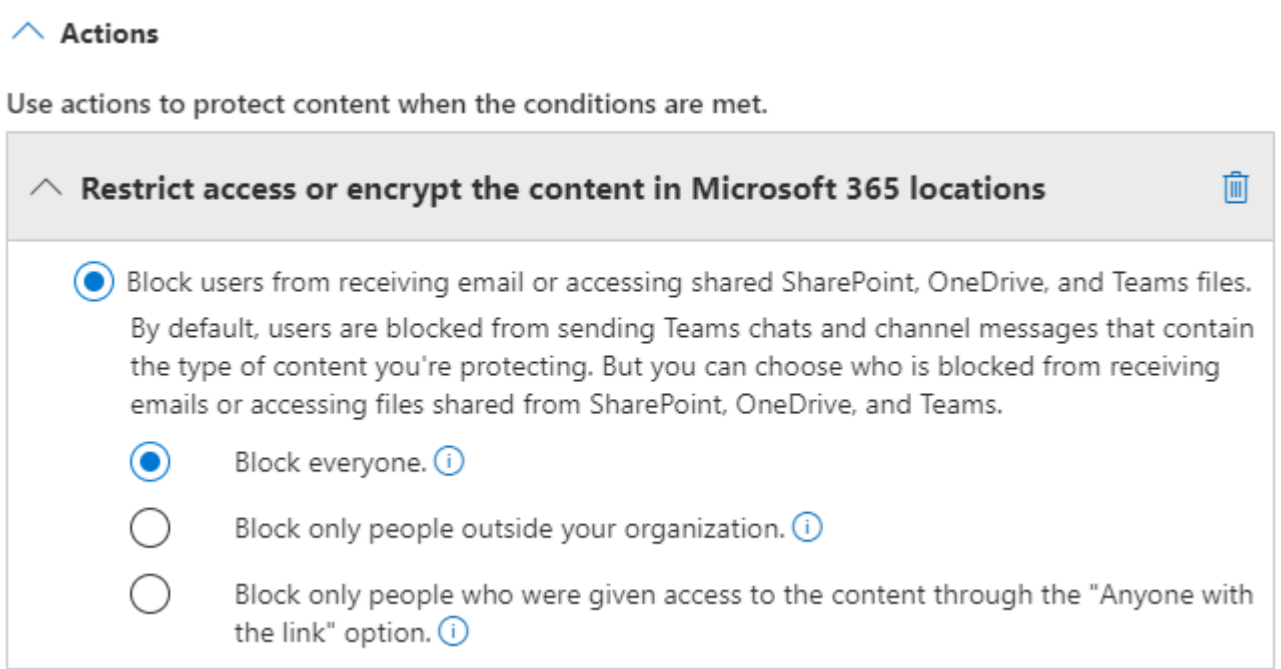
HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

Name	Member of
User1	Members group of Site1
User2	Owners group to Site1
Admin1	SharePoint Administrator role

You have a data loss prevention (DLP) policy named DLP1 as shown in the following exhibit.


Actions
Use actions to protect content when the conditions are met.
Restrict access or encrypt the content in Microsoft 365 locations
Block users from receiving email or accessing shared SharePoint, OneDrive, and Teams files.
By default, users are blocked from sending Teams chats and channel messages that contain the type of content you're protecting. But you can choose who is blocked from receiving emails or accessing files shared from SharePoint, OneDrive, and Teams.
Block everyone.
Block only people outside your organization.
Block only people who were given access to the content through the "Anyone with the link" option.

You apply DLP1 to Site1

-

User1 uploads a file named File1 to Site1. File does NOT match any of the DLP1 rules. User2 updates File1 to contain data that matches the DLP1 rules.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can access File1 on Site1.	○	○
User2 can access File1 on Site1.	○	○
Admin1 can access File1 on Site1.	○	○

Hide Answer

Suggested Answer:

Answer Area

Statements	Yes	No
User1 can access File1 on Site1.	○	●
User2 can access File1 on Site1.	●	○
Admin1 can access File1 on Site1.	●	○

by Seidor_Analytics at *Sept. 5, 2025, 8:18 a.m.*

Comments

Eltooth 2 months ago

Yes
Yes
No

1. User1 can access File1 on Site1
Answer: Yes
Explanation: User1 is a Member of Site1. DLP does not remove internal permissions; access remains intact.

2. User2 can access File1 on Site1
Answer: Yes
Explanation: User2 is an Owner of Site1. Owners retain full access unless permissions are explicitly changed.

3. Admin1 can access File1 on Site1
Answer: No
Explanation: SharePoint Administrators do not have automatic file access. They need to be added as Owner/Member.

upvoted 1 times

Caezarlay 2 months, 3 weeks ago

DLP is only blocking when try to share outside of M365 via teams or email. Normally, all users still has access as long as they are able to access SharePoint.

it should be 'Y, Y, Y'

upvoted 2 times

Caezarlay 2 months, 3 weeks ago

#Edit
It should be Y, Y, N. SharePoint administrator cannot open file directly unless they are given permission (e.g owner or member role of that site).

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 75 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 75

Topic #: 2

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 E5 subscription that uses Microsoft Purview.

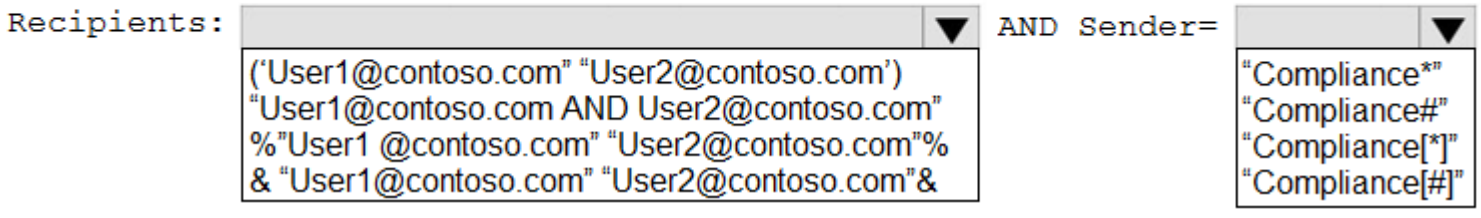
You need to perform a content search for email messages that meet the following requirements:

- Are delivered to both user1@contoso.com and user2@contoso.com
- Are sent from a user account that has a name that starts with the word Compliance

How should you complete the query in the KQL editor? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Hide Answer

Suggested Answer:

Answer Area

by Seidor_Analytics at *Sept. 5, 2025, 8:24 a.m.*

Comments

Eltooth Highly Voted 2 months, 1 week ago

Answer is not 100% accurate.
This is what the real answer is in a Purview tenant:
(recipients:user1@contoso.com AND recipients:user2@contoso.com) AND sender:Compliance*

upvoted 6 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 76 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 76

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 subscription.

You plan to retain the following audit log record types and activities for the next three years:

• CopilotInteraction: All activities selected (1/1)
o Interacted with Copilot
• ComplianceDLPEndpoint: All activities selected (2/2)
o Matched DLP rule
o Removed DLP rule from document
• AzureActiveDirectory: 2 of 25 activities selected (2/25)
o Reset user password
o Changed user password

What is the minimum number of audit retention policies you should create to retain only the selected record types and activities?

A. 1

B. 2

C. 3

D. 5

Hide Answer

Suggested Answer: *A*

Community vote distribution

B (100%)

by Leon1969 at *Nov. 1, 2025, 5:51 p.m.*

Comments

P1233 1 month ago

Selected Answer: B

COrrect answer is B. You need two policies.
CopilotInteraction and ComplianceDLPEndpoint both contain all actions and can be grouped into one policy.

AzureActiveDirectory only contains a subset (2 of 25) and needs its own policy as it does not contain all actions.

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 77 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 77

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the data loss prevention (DLP) policies shown in the following table.

Name	Priority	Rule
DLP1	0	Rule1
DLP2	1	Rule2
DLP3	2	Rule3
DLP4	3	Rule4

The DLP rules are configured as shown in the following table.

Rule	User notifications	Policy tip	If there's a match for this rule, stop processing additional DLP policies and rules
Rule1	On	Tip 1	Enabled
Rule2	On	Tip 2	Disabled
Rule3	On	Tip 3	Enabled
Rule4	On	Tip 4	Disabled

All the policies are assigned to Site1.

You need to ensure that if a user uploads a document to Site1 that matches all the rules, the user will be shown the Tip 2 policy tip.

What should you do?

A. Enable additional processing of the policies if there is a match for Rule1.

B. Prevent additional processing of the policies if there is a match for Rule2.

C. Change the priority of DLP2 to 3.

D. Change the priority of DLP2 to 0.

Hide Answer

Suggested Answer: *D*

Community vote distribution

B (100%)

by Prides at *Nov. 14, 2025, 11:19 p.m.*

Comments

Prides 4 weeks, 1 day ago

Selected Answer: B

stop additional at rule 2

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 79 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 79

Topic #: 2

[All SC-401 Questions]

HOTSPOT

-

You have a data loss prevention (DLP) policy that has the advanced DLP rules shown in the following table.

Name	Priority	Actions
Rule1	0	• Notify users with email and policy tips • User overrides: Off
Rule2	1	• Notify users with email and policy tips • Restrict access to the content • User overrides: Off
Rule3	2	• Notify users with email and policy tips • Restrict access to the content • User overrides: On
Rule4	3	• Notify users with email and policy tips • Restrict access to the content • User overrides: Off

You need to identify which rules will apply when content matches multiple advanced DLP rules.

Which rules should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

If content matches Rule1, Rule2, and Rule3:

- Only Rule1 takes effect
- Only Rule2 takes effect
- Only Rule3 takes effect
- Rule1, Rule2, and Rule3 take effect

If content matches Rule2, Rule3, and Rule4:

- Only Rule2 takes effect
- Only Rule3 takes effect
- Only Rule4 takes effect
- Rule2, Rule3, and Rule4 take effect

Hide Answer

Suggested Answer:

Answer Area
If content matches Rule1, Rule2, and Rule3:
Only Rule1 takes effect
Only Rule2 takes effect
Only Rule3 takes effect
Rule1, Rule2, and Rule3 take effect
If content matches Rule2, Rule3, and Rule4:
Only Rule2 takes effect
Only Rule3 takes effect
Only Rule4 takes effect
Rule2, Rule3, and Rule4 take effect

by Alcpt at *Nov. 12, 2025, 3 p.m.*

Comments

Alcpt 1 month ago

#1 = Rule1, no option for user to override.
The restriction is immediately enforced
User cannot bypass the restriction
No further rules are evaluated

#2 Rule 2, no option for user to override.
The restriction is immediately enforced
User cannot bypass the restriction
No further rules are evaluated

let me know what you think?

upvoted 3 times

Alcpt 1 week, 6 days ago

Sorry:
#1 = Only Rule 2 takes effect
#2 = Only Rule 2 takes effect

as per link below:
"When content is evaluated against rules, the rules are processed in priority order. If content matches multiple rules, the first rule evaluated that has the most restrictive action is enforced."
https://learn.microsoft.com/en-us/purview/dlp-policy-reference#rule-priority

upvoted 1 times

nuin01 3 weeks, 5 days ago

#1 = Only Rule 3 takes effect
#2 = Only Rule 3 takes effect
When content is evaluated against rules, the rules are processed in priority order. If content matches multiple rules, the first rule evaluated that has the most restrictive action is enforced.

upvoted 1 times

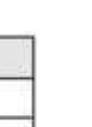
nuin01 3 weeks, 5 days ago

Sorry:
#1 = Only Rule 2 takes effect
#2 = Only Rule 2 takes effect
Rule 2 is more restrictive than Rule 3 because not allows overrides

upvoted 3 times

EXAMTOPICS

Microsoft Discussions



Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 82 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 82

Topic #: 2

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 E5 subscription that uses Microsoft Teams and contains the users shown in the following table.

Name	Team membership
User1	Team1, Team2
User2	Team2

You have the retention policies shown in the following table.

Name	Location	Included	Retain items for	Start retention period	At the end of retention period
Policy1	Microsoft Teams channel messages	All teams	7 years	When items are created	Delete items automatically
	Microsoft Teams chats	User1			
Policy2	Microsoft Teams channel messages	Team1	5 years	When items are created	Delete items automatically
	Microsoft Teams chats	User2			

The users perform the actions shown in the following table.

User	Location	Action
User1	Team1 channel	Edits a message
User2	Private 1:1 chat with User1	Sends a message to User1
User1	Team2 channel	Deletes a message

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
The message edited by User1 will be deleted after five years.	○	○
User1 can see the message sent by User2 for up to seven years.	○	○
The message deleted by User1 will be moved to the SubstrateHolds folder.	○	○

Hide Answer

Suggested Answer:

Answer Area

Statements	Yes	No
The message edited by User1 will be deleted after five years.	○	●
User1 can see the message sent by User2 for up to seven years.	○	●
The message deleted by User1 will be moved to the SubstrateHolds folder.	●	○

by 9ebaad0 at *Nov. 18, 2025, 9:55 a.m.*

Comments

9ebaad0 3 weeks, 4 days ago

The answer is NYY.
Both retention policies apply to both users & both policies are to retain and then delete so are considered a retention policies NOT deletion policies.
1. NO - Longest retention policy wins, the edited message will be deleted after 7 years
2. YES - Longest retention policy wins, the message will be seen for up to 7 years
3. YES - Retained deleted Teams chats are moved to the SubstrateHolds folder in a hidden Exchange Mailbox folder

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 83 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 83

Topic #: 2

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription.

You need to apply data loss prevention (DLP) policies to the following:

- Microsoft Exchange Online mailboxes
- Microsoft SharePoint Online sites
- Microsoft Power BI workspaces
- Microsoft OneDrive accounts
- On-premises repositories

What is the minimum number of DLP policies required to achieve the goal?

A. 1

B. 2 **Most Voted**

C. 3

D. 4

E. 5

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (67%) A (33%)

by Pavol_Misun at *Nov. 11, 2025, 2:07 p.m.*

Comments

nuin01 3 weeks, 6 days ago

Selected Answer: A

You can select all this sources in one DLP

upvoted 1 times

Pavol_Misun 1 month ago

Selected Answer: B

Policy 1: Exchange Online + SharePoint Online + OneDrive + Power BI (all cloud locations can be combined in one policy).
Policy 2: On-premises repositories (requires its own policy)

upvoted 2 times

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 85 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 85

Topic #: 2

[All SC-401 Questions]

You need to create a retention policy to retain all the files from Microsoft Teams channel conversations and private chats.

Which two locations should you select in the retention policy? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Microsoft 365 groups

B. Exchange email

C. Team channel messages

D. SharePoint sites **Most Voted**

E. OneDrive accounts **Most Voted**

F. Team chats

Hide Answer

Suggested Answer: *DE*

Community vote distribution

DE (100%)

by 9ebaad0 at *Nov. 18, 2025, 5:01 p.m.*

Comments

9ebaad0 3 weeks, 4 days ago

Selected Answer: DE

D & E are the correct answers. Files in team chats are stored in OneDrive. Files in teams channels are stored in SharePoint

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 86 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 86

Topic #: 2

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft SharePoint Online site named Site1 that contains the users shown in following table.

Name	Role
User1	Owner
User2	Member

You create the retention labels shown in the following table.

Name	Retention period	Start the retention period based on	Choose what happens after the retention period
Retention1	2 years	When items were labeled	Deactivate retention settings
Retention2	1 year	When items were labeled	Change the label to Retention1

You publish the retention labels to Site1.

Site1 contains the files shown in following table.

Name	Modified by	Retention label	Label applied
File1	User2	Retention1	August 1, 2024
File2	User1	Retention2	August 1, 2024

Which files can User1 delete on May 15, 2025, and which files can User2 delete on August 15, 2026? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Hide Answer

Suggested Answer:

by 9ebaad0 at *Nov. 18, 2025, 4:40 p.m.*

Comments

9ebaad0 3 weeks, 4 days ago

Both files can be deleted at any time. retention policies dont prevent users from deleting files. Deleted files with a retention policy attached will be kept in preservation hold

upvoted 3 times

bobg 2 weeks, 4 days ago

this is what makes these questions so awkward. They should be clearer in their definition of deleted in the question.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 87 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 87

Topic #: 2

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Role
User1	Global Administrator
User2	Compliance Administrator

You have a retention policy that has the following configurations:

- Retain items for a specific period: 5 years
- Locations to apply the policy: Exchange email, SharePoint sites

You place a Preservation Lock on Policy1.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can remove Exchange email from the locations in Policy1.	○	○
User2 can increase the retention period to seven years in Policy1.	○	○
User1 can decrease the retention period to three years in Policy1.	○	○

Hide Answer

Suggested Answer:

Answer Area

Statements	Yes	No
User1 can remove Exchange email from the locations in Policy1.	○	■
User2 can increase the retention period to seven years in Policy1.	■	○
User1 can decrease the retention period to three years in Policy1.	○	■

by Alcpt at *Nov. 30, 2025, 2:16 p.m.*

Comments

Alcpt 1 week, 6 days ago

answer is correct

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 88 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 88

Topic #: 2

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft SharePoint Online site named Site1 that contains the files shown in the following table.

Name	Number of IP addresses in the file
File1.txt	2
File2.docx	6
File3.dat	4

You have a data loss prevention (DLP) policy named DLP1 that has the advanced DLP rules shown in the following table.

Name	Content contains	Policy tip	Priority
Rule1	1 or more IP addresses	Tip1	0
Rule2	2 or more IP addresses	Tip2	1
Rule3	6 or more IP addresses	Tip3	2

You apply DLP1 to Site1.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

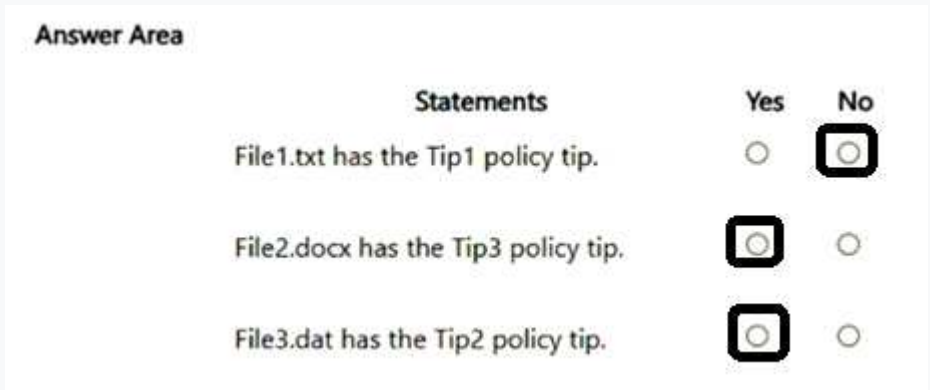
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
File1.txt has the Tip1 policy tip.	○	○
File2.docx has the Tip3 policy tip.	○	○
File3.dat has the Tip2 policy tip.	○	○

Hide Answer

Suggested Answer:



by bobg at *Nov. 26, 2025, 9:27 a.m.*

Comments

bobg 2 weeks, 3 days ago

I think they all get Tip1 as every file has 1 more more ip address? So YNN.

upvoted 2 times

Alcpt 1 week, 6 days ago

You are correct, Tip 1 always applies.
The confusion arises because people expect the "most specific" rule to apply, but in DLP, it's strictly about priority order, not specificity of conditions.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 89 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 89

Topic #: 2

[All SC-401 Questions]

HOTSPOT

-

You create a retention policy as shown in the following exhibit.

Retention Policy1

Status

Enabled (Success)

Description

Retention policy for SharePoint Site1 and Exchange

Applies to content in these locations

Exchange email
SharePoint sites

Settings

Retention period

Keep content, and delete it if it's older than 10 years

Preservation lock

No

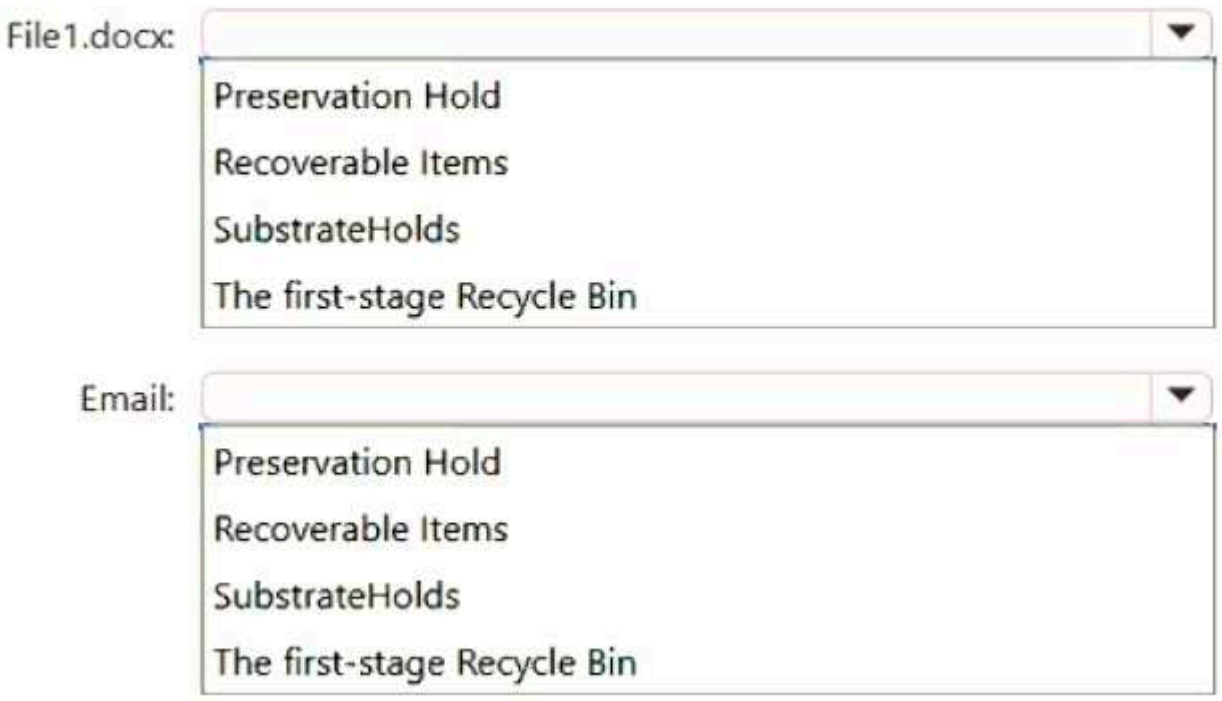
A user named User1 deletes a file named File1.docx from a Microsoft SharePoint Online site named Site1.

A user named User2 deletes an email and empties the Deleted Items folder in Microsoft Outlook.

Where is the content retained one year after deletion? To answer, select the appropriate options in the answer area.

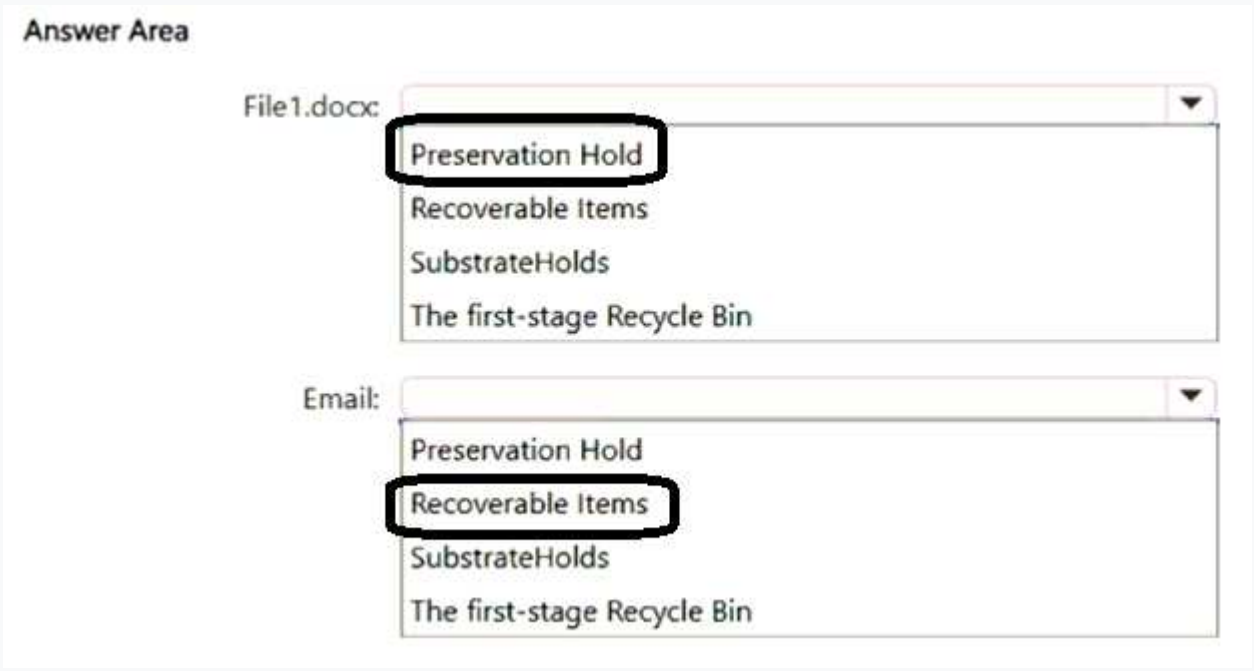
NOTE: Each correct selection is worth one point.

Answer Area



Hide Answer

Suggested Answer:



by bobg at *Nov. 26, 2025, 9:36 a.m.*

Comments

bobg 2 weeks, 3 days ago

Preservation Hold and SubstrateHolds i think here.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 90 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 90

Topic #: 2

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
User1	Information Protection Administrator
User2	Information Protection Analyst
User3	Information Protection Investigator

You need to delegate the following tasks:

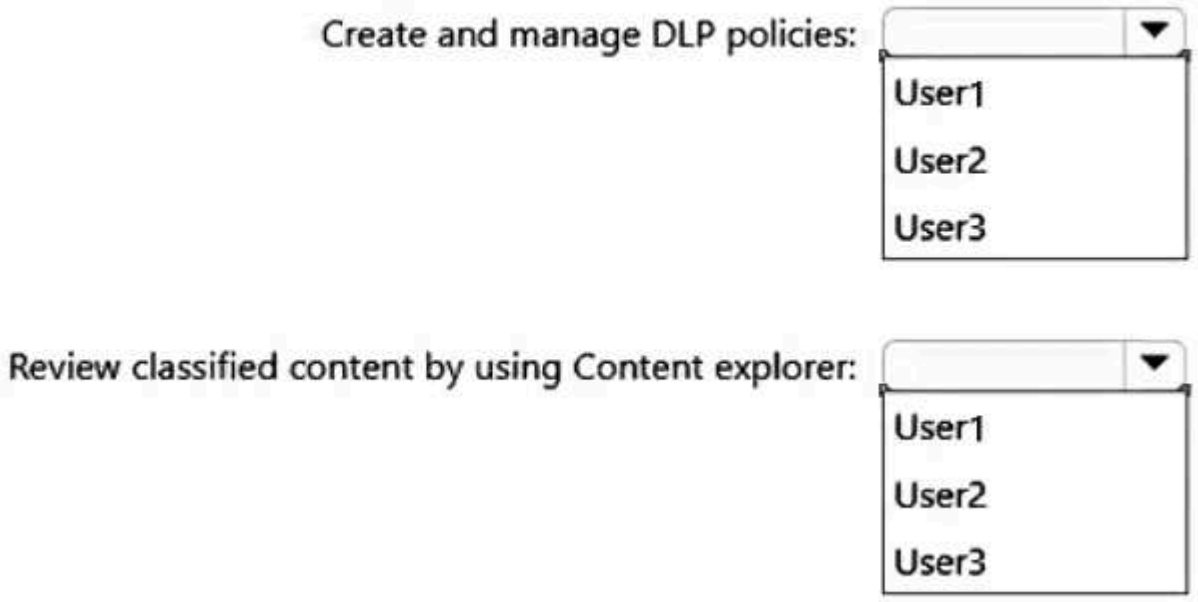
- Create and manage data loss prevention (DLP) policies.
- Review classified content by using Content explorer.

The solution must use the principle of least privilege.

Which user should perform each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Hide Answer

Suggested Answer:

by bobg at *Nov. 26, 2025, 9:40 a.m.*

Comments

bobg 2 weeks, 3 days ago

User 1 and User2. Analyst gives enough permissions to view classified content. Investigator has additional permissions.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 91 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 91

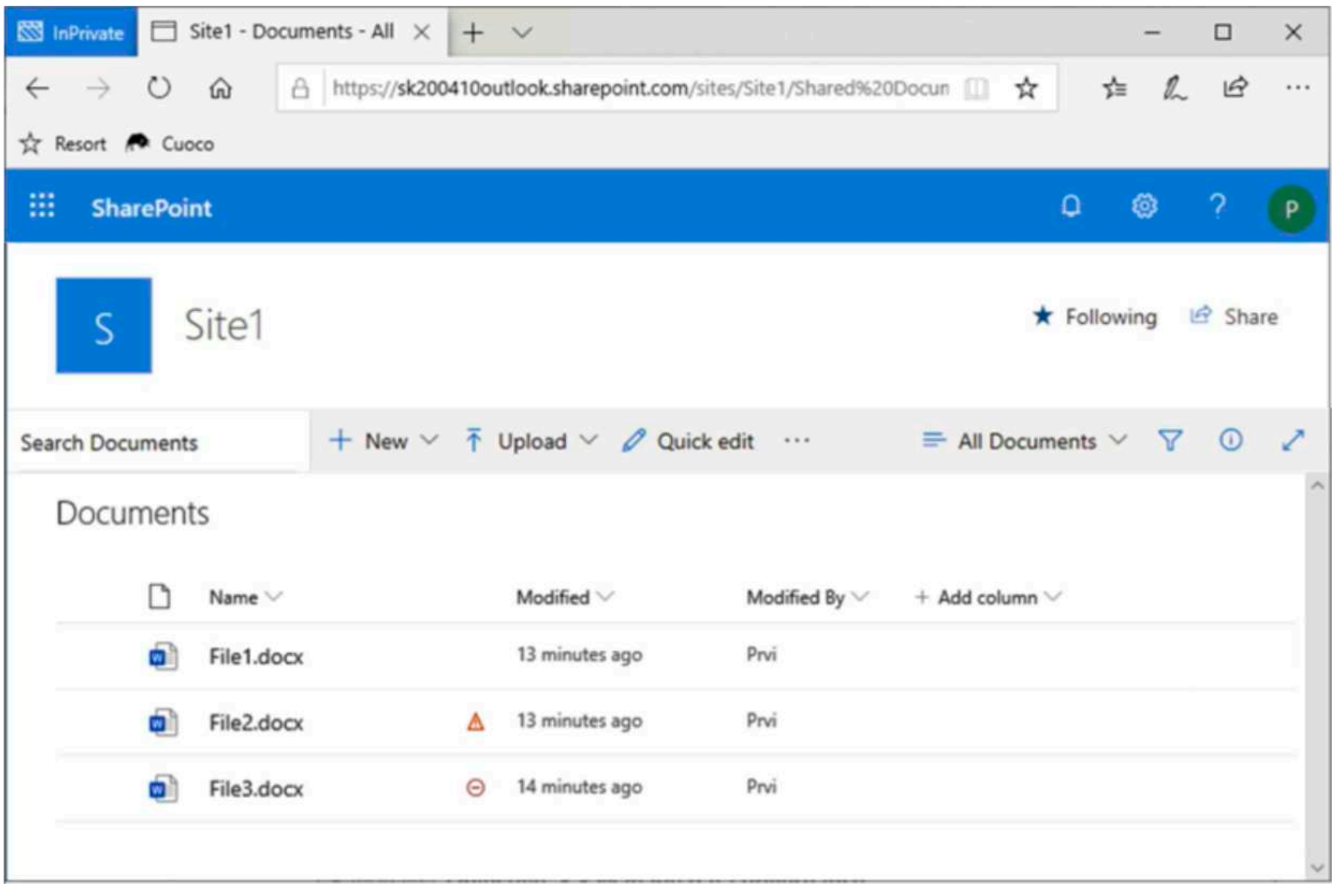
Topic #: 2

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 E5 tenant that contains two users named User1 and User2 and a Microsoft SharePoint Online site named Sitel as shown in the following exhibit.



For Site1, the users are assigned the roles shown in the following table.

Name	Role
User1	Owner
User2	Member

You publish a retention label named Retention1 to Site1.

To which files can the users apply Retention1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1:
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

User2:
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

Hide Answer

Suggested Answer:

Answer Area

User1:
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

User2:
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

by 9ebaad0 at *Nov. 18, 2025, 4:56 p.m.*

Comments

Alcpt 1 week, 6 days ago

Geez, I think:
user1 can apply to File1 only as this file has synced successfully,
user2 can apply to File 1 only as this file has synced successfully,
NOT File 2. The sync issues. When a file has a sync conflict (orange triangle), it's typically placed in a locked or read-only state by the OneDrive sync client. This prevents any metadata changes, including applying retention labels, until the conflict is resolved
NOT file 3. The red circle indicates a complete sync failure as the file content never successfully uploaded to SharePoint. What you see in the document library is essentially a broken placeholder or stub file. There is no valid SharePoint list item to attach the retention metadata to.

upvoted 1 times

Alcpt 3 days, 23 hours ago

correction:
User1: File1.docx, File2.docx, and File3.docx
User2: File1.docx only

upvoted 1 times

9ebaad0 3 weeks, 4 days ago

personally i think it is file 1 & 2 for both as the symbol on file 3 shows the file has failed to sync to sharepoint and isnt in the cloud and so cannot have a retention label applied.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 92 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 92

Topic #: 2

[All SC-401 Questions]

SIMULATION

-

Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and select the username below.

To enter your password, place your cursor in the Enter password box and select the password below.

Microsoft 365 Username:
admin@WWLx121586.onmicrosoft.com

Microsoft 365 Password: XXXXXXXXX

If the Microsoft Edge browser or Microsoft 365 portal does not load successfully, select the Microsoft Edge browser icon from the task bar, type the URL “https://admin.microsoft.com”, and press Enter.

The following information is for technical support purposes only:

Lab Instance: XXXXXXXXX

-

Task 1

-

You plan to implement Endpoint data loss prevention (Endpoint DLP). You plan to create a policy that will restrict OneDrive.exe from accessing

files that have the Highly Confidential sensitivity label.

You need to configure the Endpoint DLP settings so that onedrive.exe actions can be restricted by a DLP policy.

You do NOT need to create a DLP policy at this time.

Hide Answer

Suggested Answer:

To restrict onedrive.exe actions in Microsoft Purview, you first configure it as a restricted app group in Endpoint DLP settings and then add that group to a DLP policy in the Microsoft Purview portal. In the Endpoint DLP settings, navigate to Data loss prevention > Settings > Data loss prevention > Endpoint settings > Restricted apps and app groups. Create a new group called "Cloud Sync apps," select the Auto-quarantine option, and add onedrive.exe as the executable name for Windows.

Configure the restricted app group
Step 1: Sign in to the Microsoft Purview portal.

Step 2: Go to Data loss prevention > Settings (gear icon) > Data loss prevention > Endpoint settings.

Step 3: Expand Restricted apps and app groups.

Step 4: Under "Restricted app groups," select Add restricted app group.

Step 5: Enter a group name, such as Cloud Sync apps.

Step 6: Check the box for Auto-quarantine.

Step 7: In the "App name" field, add the executable name:
For Windows, enter onedrive.exe and click the + button.

Reference:
https://learn.microsoft.com/en-us/purview/endpoint-dlp-using

by bobg at *Nov. 26, 2025, 9:59 a.m.*

Comments

bobg 2 weeks, 3 days ago

I think you can add a restricted app instead of a restricted app group in the same location?

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 2 QUESTION 94 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 94

Topic #: 2

[All SC-401 Questions]

SIMULATION

-

Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and select the username below.

To enter your password, place your cursor in the Enter password box and select the password below.

Microsoft 365 Username:

admin@WWLx121586.onmicrosoft.com

Microsoft 365 Password: XXXXXXXXX

If the Microsoft Edge browser or Microsoft 365 portal does not load successfully, select the Microsoft Edge browser icon from the task bar, type the URL “https://admin.microsoft.com”, and press Enter.

The following information is for technical support purposes only:

Lab Instance: XXXXXXXXX

-

Task 4

-

You need reduce the number of false-positives generated by the General Data Protection Regulation (GDPR) data loss prevention (DLP) policy.

Hide Answer

Suggested Answer:

To reduce false-positives with a GDPR DLP policy, run the policy in audit-only mode first to identify issues, continuously refine the rules based on this data, and train employees on proper data handling.

To run an existing GDPR DLP policy in audit mode, you need to edit the policy in your Microsoft Purview portal and set the policy mode to "simulation" or "test". In the policy configuration, select the option to "Run the policy in simulation mode" or "Test mode" instead of enabling enforcement immediately. This will log any violations without blocking them, allowing you to review the results before a full deployment.

Steps to run a policy in audit (simulation) mode

Step 1: Navigate to DLP policies: Sign in to the Microsoft Purview portal and go to Data loss prevention > Policies.

Step 2: Edit the policy: Select the existing GDPR policy you want to run and choose to edit it.

Step 3: Locate the policy mode settings: In the policy configuration workflow, find the page for policy mode, which may be labeled as "Policy Mode" or "Simulate or turn on the policy".

Step 4: Enable simulation mode: Choose the option to "Run the policy in simulation mode".

Step 5: Configure optional settings: You can also choose to "Show policy tips" in simulation mode to help educate users about potential violations without actually blocking them. [Skip]

Step 6: Save and submit: Proceed through the rest of the wizard and select Next and Submit to save your changes.

Reference:
https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp

by bobg at *Nov. 28, 2025, 9:30 a.m.*

Comments

bobg 2 weeks, 1 day ago

Go to Microsoft Purview → Data Loss Prevention

Open the GDPR DLP policy

Edit the rules

Expand Conditions

For the sensitive info types:

Increase accuracy requirements

Increase confidence level

Require multiple evidence types

Increase min. instance count

Save and republish the policy

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 1 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 1
Topic #: 3
[All SC-401 Questions]

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You recently discovered that the developers at your company emailed Azure Storage Account keys in plain text to third parties.
You need to ensure that when Azure Storage Account keys are emailed, the emails are encrypted.
Solution: You configure a mail flow rule that matches the text patterns.
Does this meet the goal?

A. Yes **Most Voted**

B. No

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (60%) A (40%)

by 337257e at *Sept. 19, 2025, 10:50 p.m.*

Comments

P1233 1 month ago

Selected Answer: B

You can use a rule with a SIT, not a textpattern. It is to unsecure.

upvoted 1 times

Eltooth 2 months ago

Selected Answer: B

B is correct answer.
A mail flow rule that matches text patterns is not reliable for detecting Azure Storage Account keys because:

Keys have complex formats that are better detected using Sensitive Information Types (SITs) or custom SITs.
Text pattern matching in mail flow rules is prone to false positives and negatives.
Even if the rule matches some patterns, it does not guarantee accurate detection of all keys, which is critical for compliance.
The correct approach is to use:

A mail flow rule or DLP policy that matches a Sensitive Information Type (built-in or custom for Azure Storage keys).
Then apply encryption using Microsoft Purview Message Encryption or a sensitivity label.

upvoted 2 times

Eltooth 2 months, 2 weeks ago

Selected Answer: A

A is correct answer: Yes
By configuring a mail flow rule (also known as a transport rule) in Microsoft Exchange Online that detects specific text patterns (e.g., Azure Storage Account keys), you can apply email encryption automatically when such content is detected. This helps prevent sensitive information from being sent in plain text.

However, for this to be effective:
The rule must accurately match the format of the keys (e.g., using regular expressions).
The rule must be configured to apply encryption (such as Microsoft Purview Message Encryption).
Users must not circumvent the rule by altering the format or using attachments.

upvoted 1 times

Eltooth 2 months ago

Actually on reflection this would be B - No.
Here's why:

A mail flow rule that matches text patterns is not reliable for detecting Azure Storage Account keys because:

Keys have complex formats that are better detected using Sensitive Information Types (SITs) or custom SITs.
Text pattern matching in mail flow rules is prone to false positives and negatives.

Even if the rule matches some patterns, it does not guarantee accurate detection of all keys, which is critical for compliance.

✅ The correct approach is to use:

A mail flow rule or DLP policy that matches a Sensitive Information Type (built-in or custom for Azure Storage keys).
Then apply encryption using Microsoft Purview Message Encryption or a sensitivity label.

upvoted 1 times

337257e 2 months, 3 weeks ago

Selected Answer: A

a is answ3r

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 2 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 2

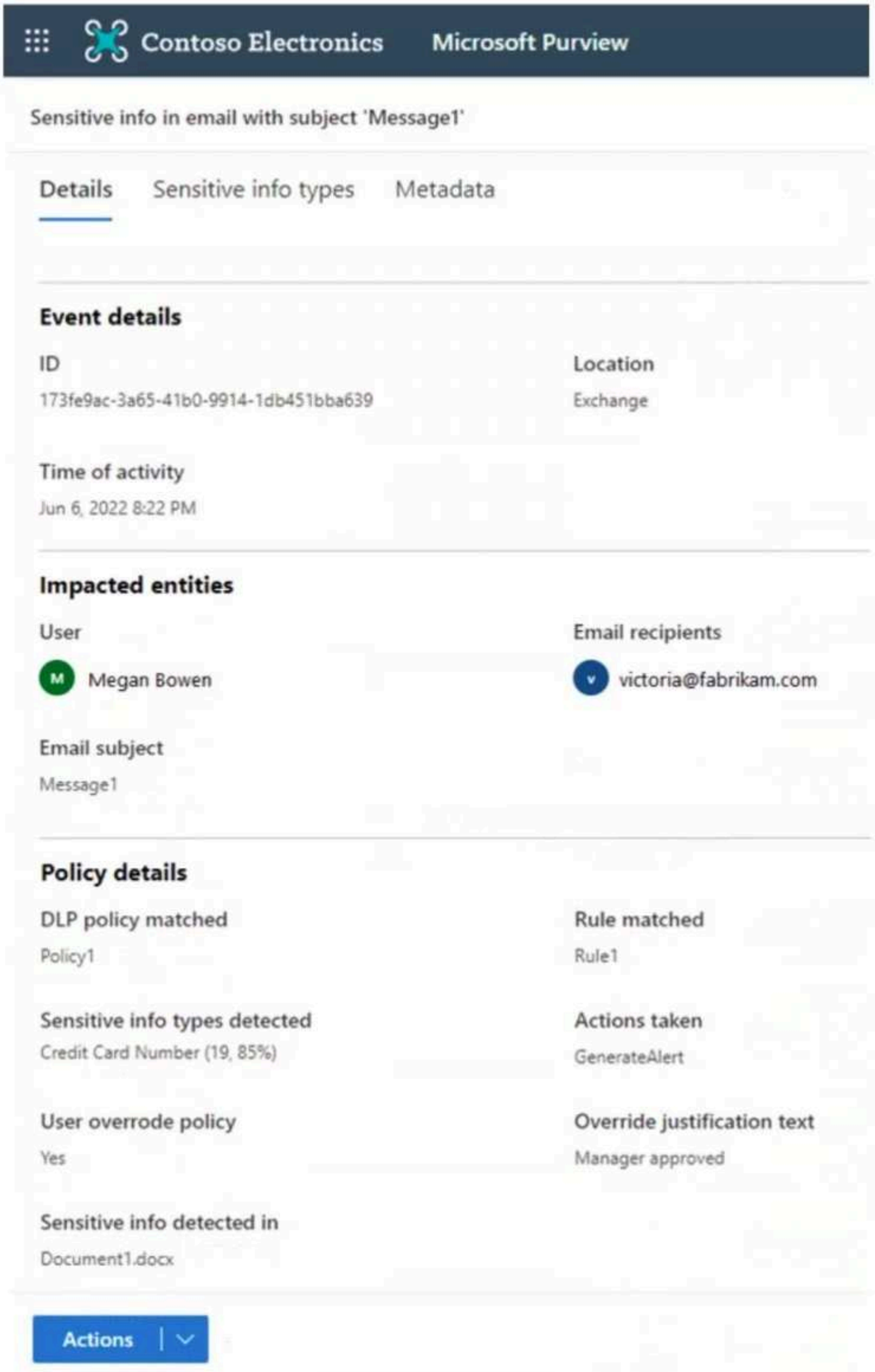
Topic #: 3

[All SC-401 Questions]

HOTSPOT -

You have a Microsoft 365 E5 subscription.

You receive the data loss prevention (DLP) alert shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

The email was **[answer choice]**.

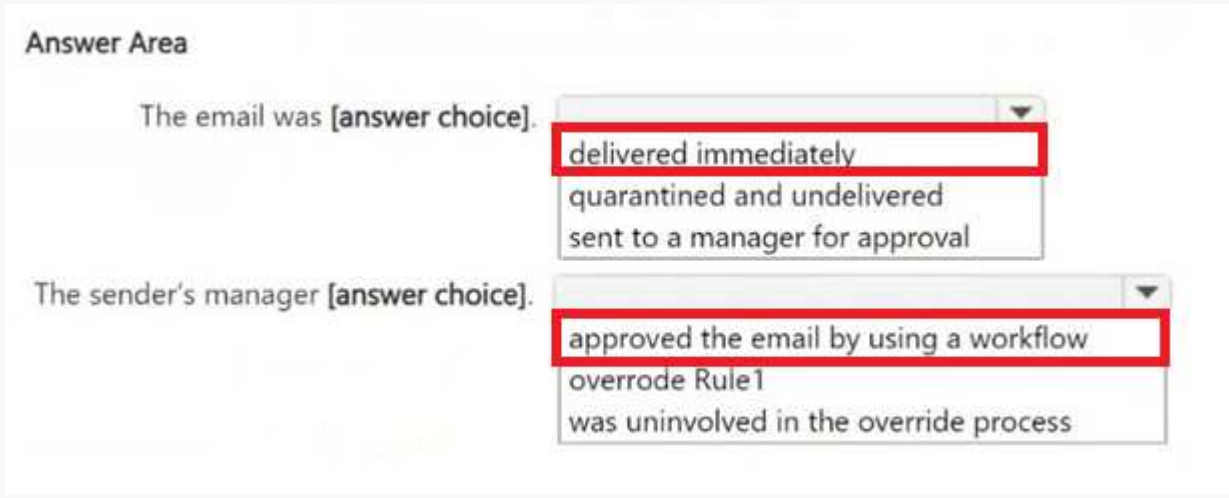
- delivered immediately
- quarantined and undelivered
- sent to a manager for approval

The sender's manager **[answer choice]**.

- approved the email by using a workflow
- overrode Rule1
- was uninvolved in the override process

Hide Answer

Suggested Answer:


Answer Area
The email was [answer choice].
delivered immediately
quarantined and undelivered
sent to a manager for approval
The sender's manager [answer choice].
approved the email by using a workflow
overrode Rule1
was uninvolved in the override process

by PsiCzar at *June 5, 2025, 5:52 a.m.*

Comments

PsiCzar Highly Voted 6 months, 1 week ago

The answer given is incorrect. "User overrode policy" is set to yes, and the reason they gave was "Manager approved". The correct answer is "delivered immediately" and "was uninvolved in the override process".

upvoted 20 times

zied01 4 months, 4 weeks ago

yes you are right , the override was maded by the end user him self without the approval of anybody else

upvoted 3 times

deeptha92 Most Recent 3 months, 2 weeks ago

"Approved by the manager" is just a justification user gave, Real manager was not involved.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 3 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 3

Topic #: 3

[All SC-401 Questions]

HOTSPOT -

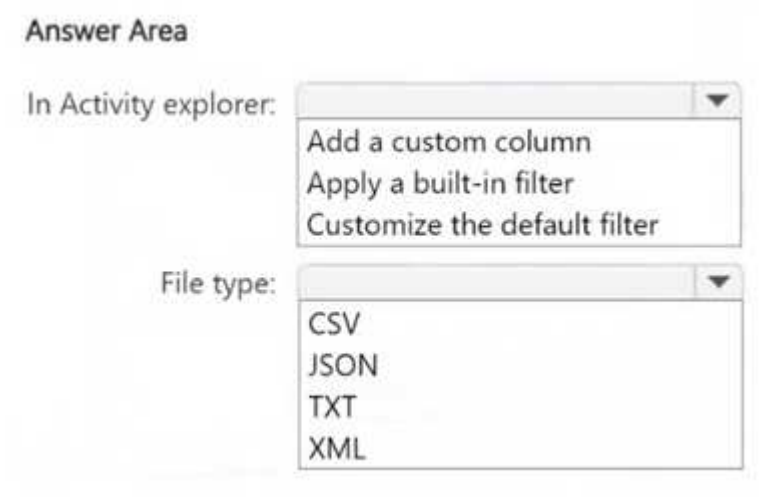
You have a Microsoft 365 E5 subscription that has data loss prevention (DLP) implemented.

You plan to export DLP activity by using Activity explorer.

The exported file needs to display the sensitive info type detected for each DLP rule match.

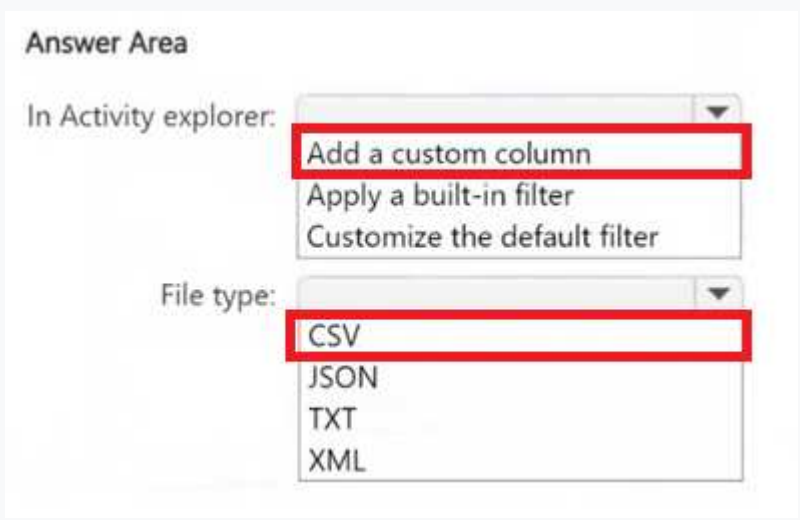
What should you do in Activity explorer before exporting the data, and in which file format is the file exported? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Hide Answer

Suggested Answer:



by examtopicssc401 at *June 14, 2025, 4:12 p.m.*

Comments

Eltooth 2 months, 3 weeks ago

Custom column
CSV

upvoted 2 times

ppolychron 4 months, 1 week ago

Answer is correct. Tested in lab.

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 4 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 4

Topic #: 3

[All SC-401 Questions]

DRAG DROP -

You have a Microsoft 365 subscription that contains 20 data loss prevention (DLP) policies.

You need to identify the following:

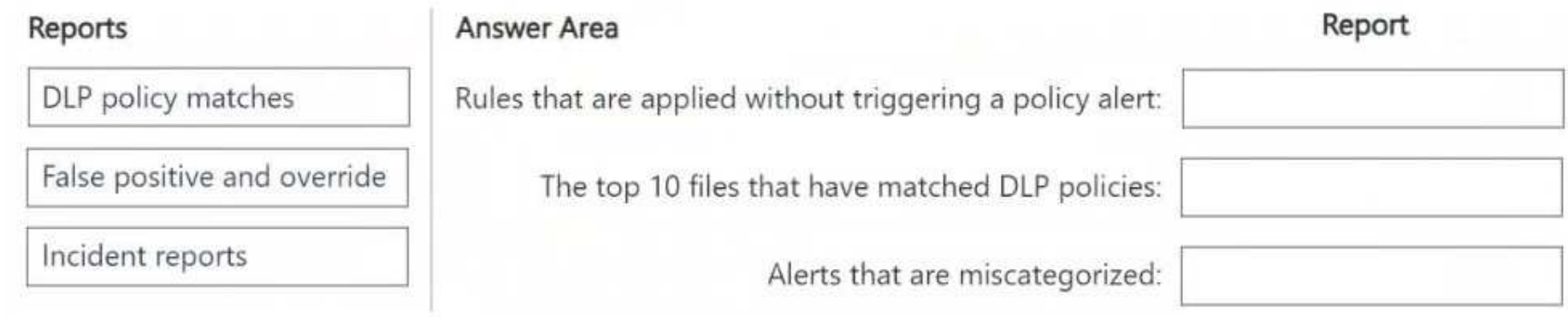
Rules that are applied without triggering a policy alert

The top 10 files that have matched DLP policies

Alerts that are miscategorized -

Which report should you use for each requirement? To answer, drag the appropriate reports to the correct requirements. Each report may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Hide Answer

Suggested Answer:

Answer Area
Report
Rules that are applied without triggering a policy alert:
False positive and override
The top 10 files that have matched DLP policies:
DLP policy matches
Alerts that are miscategorized:
Incident reports

by SH_Train at *June 11, 2025, 11:53 p.m.*

Comments

Lix0u Highly Voted 5 months, 2 weeks ago

DLP matches
incident reports
false positive and override

upvoted 7 times

ppolychron Most Recent 4 months, 1 week ago

With the introduction of the new Purview Portal I think things have changed a little.
I will go with:
DLP policy matches (From Activity Explorer)
DLP policy matches (From Activity Explorer, export dlp matches to csv, analyze in Excel)
DLP incident reports (From Defender Portal)

upvoted 1 times

Koenst 5 months, 3 weeks ago

DLP polcy matches
DLP polcy matches
False positive and override

upvoted 2 times

58d4802 6 months ago

The answer provided is partially correct. The better answer is:
DLP policy matches
DLP policy matches
DLP incident reports

upvoted 1 times

SH_Train 6 months ago

Does anyone know where these particular reports are located? For these requirements i am looking at Activity Explorer and DLP Alerts?

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 5 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 5

Topic #: 3

[All SC-401 Questions]

HOTSPOT -

You have a Microsoft 365 E5 subscription. The subscription contains devices that are onboarded to Microsoft Purview and configured as shown in the following table.

Name	Operating system	Microsoft Purview browser extension
Device1	Windows 11	Installed
Device2	Windows 11	Not installed
Deivce3	macOS	Installed

The subscription contains the users shown in the following table.

Name	Activity performed during the last seven days	On device
User1	Used a generative AI website to generate an image	Device1
User2	Asked Microsoft 365 Copilot to summarize a document	Device2
User3	Browsed sample content on a generative AI website	Device3

You need to review the activities.

What should you use for each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1:
- Activity explorer in Data Security Posture Management for AI (DSPM for AI)
- Audit log search
- Insider risk audit log
- Unified Catalog

User2:
- Activity explorer in Data Security Posture Management for AI (DSPM for AI)
- Audit log search
- Insider risk audit log
- Unified Catalog

User3:
- Activity explorer in Data Security Posture Management for AI (DSPM for AI)
- Audit log search
- Insider risk audit log
- Unified Catalog

Hide Answer

Suggested Answer:

Answer Area
User1:
Activity explorer in Data Security Posture Management for AI (DSPM for AI)
Audit log search
Insider risk audit log
Unified Catalog
User2:
Activity explorer in Data Security Posture Management for AI (DSPM for AI)
Audit log search
Insider risk audit log
Unified Catalog
User3:
Activity explorer in Data Security Posture Management for AI (DSPM for AI)
Audit log search
Insider risk audit log
Unified Catalog

by PsiCzar at *June 6, 2025, 3:40 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

Activity Explorer
Audit Log - no Purview browser extension installed
Activity Explorer

upvoted 2 times

RickySmith 2 months, 3 weeks ago

User1: Activity explorer in DSPM for AI
Since the extension is installed, web activity on generative AI sites is captured by Activity explorer in Data Security Posture Management for AI (DSPM for AI).

User2: Activity explorer in DSPM for AI
If something is done in Microsoft 365 Copilot/Chat, it can be found in "Activity explorer in DSPM for AI" irrespective of the Purview extension being installed.

User3: Activity explorer in DSPM for AI
Even on macOS, if the Purview browser extension is installed, AI website activity is captured in DSPM for AI Activity Explorer.

upvoted 2 times

gabbinu 3 months, 3 weeks ago

User1: Activity explorer in DSPM for AI
Since the extension is installed, web activity on generative AI sites is captured by Activity explorer in Data Security Posture Management for AI (DSPM for AI).

User2: Audit log search
Copilot activities are not tracked by DSPM browser extension, but they are logged in Audit logs (Microsoft 365 audit logs).

User3: Activity explorer in DSPM for AI
Even on macOS, if the Purview browser extension is installed, AI website activity is captured in DSPM for AI Activity Explorer.

upvoted 2 times

ppolychron 4 months, 1 week ago

User 1: Activity Explorer in DSPM for AI
User 2: Audit Log
User 3: Activity Explorer in DSPM for AI

For User 1: We assume Edge or Chrome/Firefox with Purview Extension is used. Other browsers should be blocked.

For User 3: We assume Edge is used (No chrome or Firefox support). Other browsers should be blocked.

https://learn.microsoft.com/en-us/purview/dlp-chrome-get-started
https://learn.microsoft.com/en-us/purview/dlp-firefox-extension-get-started
https://learn.microsoft.com/en-us/purview/dlp-configure-endpoint-settings#unallowed-browsers

upvoted 1 times

liaam 4 months, 3 weeks ago

The Microsoft Purview Browser Extension is not supported on macOS.

upvoted 2 times

PsiCzar 6 months, 1 week ago

Appears to be correct. DSPM for AI requires the browser extension to be installed to detect 3rd-party AI interactions.
https://learn.microsoft.com/en-us/purview/ai-microsoft-purview-considerations

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 6 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 6

Topic #: 3

[All SC-401 Questions]

HOTSPOT -

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

You create the audit retention policies shown in the following table.

Priority	Policy name	Record type	Activities	Users	Duration
10	AuditRetention1	ExchangeItem	MailboxLogin	*None*	90 Days
20	AuditRetention2	ExchangeItem	Send, MailItemsAccesssed	User1	9 Months
30	AuditRetention3	Sharepoint	*None*	User1	6 Months
40	AuditRetention4	Sharepoint	SiteRenamed	User1	9 Months
50	AuditRetention5	Sharepoint	SiteRenamed	*None*	10 Years

The users perform the following actions:

User1 renames a Microsoft SharePoint Online site.

User2 sends an email message.

How long will the audit log records be retained for each action? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

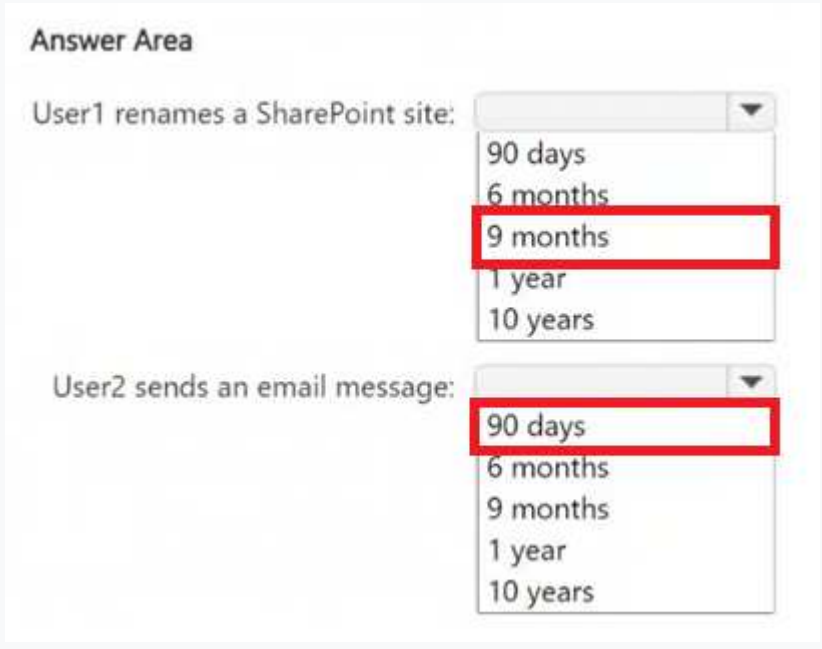
Answer Area

User1 renames a SharePoint site:
- 90 days
- 6 months
- 9 months
- 1 year
- 10 years

User2 sends an email message:
- 90 days
- 6 months
- 9 months
- 1 year
- 10 years

Hide Answer

Suggested Answer:



by leprechaun at *June 3, 2025, 9:30 a.m.*

Comments

leprechaun Highly Voted 6 months, 1 week ago

User1 renames a SharePoint site
Matching policy: AuditRetention4

Record type: SharePoint

Activity: SiteRenamed

User: User1

Retention: 9 months

Priority: 40 (higher than AuditRetention5 which is general)

Correct Answer: 9 months

User2 sends an email message
Activity: Send (ExchangeItem)

AuditRetention2 has the activity, but only applies to User1, not User2

No other ExchangeItem policy matches Send for User2

Default retention applies, which in Microsoft 365 E5 is:

Default audit log retention for ExchangeItem (E5 license): 1 year

Correct Answer: 1 year

upvoted 21 times

Alcpt 1 week, 6 days ago

User 1 = 6 months because RP3 applies as NONE = ALL ACTIONS and has a priority of 30, over RP4 and RP5.
User 2:
None RP1 nor RP2 refer to both Exchange AND User2 combinations, so the default = 1 year.

upvoted 1 times

evrybobry Most Recent 1 month ago

6 months
6 months - The default audit log retention policy only applies to audit records for activity performed by users who are assigned an Office 365 or Microsoft 365 E5 license or have a Microsoft Purview Suite (formerly known as Microsoft 365 E5 Compliance) or E5 eDiscovery and Audit add-on license. If you have non-E5 users or guest users in your organization, their corresponding audit records are retained for 180 days.

upvoted 2 times

SH_Train 6 months ago

When User1 renames a Sharepoint site, the audit retention period will be 6 months as policy AuditRetention3 is a higher priority. If the record type is selected (Sharepoint) and no activities are selected (SiteRenamed), then this policy will apply to all activities for the selected record types.

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 7 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 7

Topic #: 3

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Description
User1	• User 1 is a regional manager. • User1 is assigned the Reader role. • Three department managers report to User1.
User2	• User2 is the human resources (HR) department manager. • User2 has no Microsoft Entra roles assigned. • Five HR department users report to User2.
User3	• User3 is a developer. • User3 reports to User2. • User3 is the only user in the compliance department. • User3 is assigned the Compliance Administrator role.
User4	• User4 is the assistant of User1. • User4 has no Microsoft Entra roles assigned. • User4 handles a high volume of confidential data on behalf of User1.

Which users will Microsoft Purview insider risk management flag as potential high-impact users?

A. User1 and User2 only

B. User2 and User3 only

C. User1, User2, and User3 only

D. User1, User2, User3, and User4 **Most Voted**

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (100%)

by PsiCzar at *June 9, 2025, 4:03 a.m.*

Comments

PsiCzar Highly Voted 6 months, 1 week ago

Selected Answer: D

I think its correct because of this article.
https://techcommunity.microsoft.com/blog/microsoft-security-blog/detecting-and-investigating-security-risks-with-new-capabilities-from-insider-ri/3648940

Insider Risk Management will now be able to help security admins to prioritize alerts for potential high-impact users with our new risk booster score capabilities. By turning on this new risk booster score in Settings, using advanced machine learning algorithms the alerts for users found to have potentially higher impact will have a higher priority alert in the dashboard. This high-priority user is determined by their frequency of accessing higher sensitivity content, like sensitive information types, labels, or priority content, compared with others in the organization, and if they are a leader in the organization, depending on their role designation within Azure AD, or level of influence as configured by Azure AD.

upvoted 5 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 8 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 8

Topic #: 3

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription.

You need to review a Microsoft 365 Copilot usage report.

From where should you review the report?

A. Information Protection in the Microsoft Purview portal

B. the Microsoft 365 admin center **Most Voted**

C. DSPM for AI in the Microsoft Purview portal

D. the Microsoft Defender portal

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (100%)

by dache at *June 9, 2025, 10:25 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

Selected Answer: B

B is correct answer. Microsoft 365 admin center

upvoted 1 times

Jarem 6 months ago

Selected Answer: B

Admin 365 portal/Usage and Microsoft 365 portal/copilot

upvoted 2 times

dache 6 months, 1 week ago

Selected Answer: B

Copilot: The correct answer is: B. the Microsoft 365 admin center.
To review the Microsoft 365 Copilot usage report:
- Go to the Microsoft 365 admin center.

- Navigate to Reports > Usage.
- Select Copilot to view adoption and usage metrics.

The admin center provides insights into how Copilot is being used across your organization, helping you track engagement and effectiveness.

Data Security Posture Management (DSPM) for AI in the Microsoft Purview portal provides insights into AI usage, but it focuses on security and compliance rather than standard usage metrics.

https://learn.microsoft.com/en-us/purview/ai-microsoft-purview

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 9 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 9

Topic #: 3

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft Purview insider risk management.

You implement the HR data connector.

You need to prepare the data that will be imported by the data connector.

In which format should you prepare the data?

A. JSON

B. CSV **Most Voted**

C. TSV

D. XML

E. PRN

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (100%)

by PsiCzar at *June 9, 2025, 4:05 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

Selected Answer: B

B is correct answer.

upvoted 2 times

RickySmith 3 months, 2 weeks ago

Selected Answer: B

https://learn.microsoft.com/en-us/purview/import-hr-data

upvoted 2 times

PsiCzar 6 months, 1 week ago

Selected Answer: B

Correct.

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 10 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 10

Topic #: 3

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription.

You plan to implement insider risk management for users that manage sensitive data associated with a project.

You need to create a protection policy for the users. The solution must meet the following requirements:

Minimize the impact on users who are NOT part of the project.

Minimize administrative effort.

What should you do first?

A. From the Microsoft Purview portal, create an insider risk management policy.

B. From the Microsoft Entra admin center, create a security group.

C. From the Microsoft Entra admin center, create a User risk policy.

D. From the Microsoft Purview portal, create a priority user group. **Most Voted**

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (65%) B (35%)

by dache at *June 8, 2025, 2:08 a.m.*

Comments

dache **Highly Voted** 6 months, 1 week ago

Selected Answer: D

Copilot:
The correct answer is: D. From the Microsoft Purview portal, create a priority user group.
Creating a priority user group allows you to focus insider risk management policies on specific users who handle sensitive project data, minimizing the impact on users who are not part of the project. This approach also reduces administrative effort by ensuring that policies apply only to relevant individuals rather than the entire organization.
Once the priority user group is set up, you can then create an insider risk management policy tailored to their activities and data sensitivity.

upvoted 7 times

dache 6 months, 1 week ago

If EntraID sec group created, Copilot: Good question! While creating a security group in Microsoft Entra ID can help with managing permissions and access, it doesn't provide the specific insider risk management capabilities needed for this scenario.

upvoted 2 times

Eltooth Most Recent 2 months, 3 weeks ago

Selected Answer: D

D is correct. https://learn.microsoft.com/en-us/purview/insider-risk-management-settings-priority-user-groups#create-a-priority-user-group

upvoted 2 times

454252dfr 4 months, 1 week ago

Selected Answer: B

To meet the requirements of applying the policy only to a subset of users and minimizing administration, the first logical and most efficient step is to create a security group in Microsoft Entra ID. This group will serve as the scope for the internal risk management policy.

upvoted 1 times

ppolychron 4 months, 1 week ago

Selected Answer: D

No need to have a security group. You can add mail enabled user during the creation of the priority group.

https://learn.microsoft.com/en-us/purview/insider-risk-management-settings-priority-user-groups#create-a-priority-user-group

"On the Choose members page, select Choose members to search and select which mail-enabled user accounts are included in the group or select the Select all checkbox to add all users in your organization to the group. Select Add to continue."

upvoted 4 times

58d4802 6 months ago

Selected Answer: B

You can only create a priority user group from an existing security group — so you still need to do step B first.

upvoted 4 times

Jarem 6 months ago

Selected Answer: B

B. From the Microsoft Entra admin center, create a security group.
Creating a security group in the Microsoft Entra admin center allows you to specifically target the users who manage sensitive data associated with the project. This approach minimizes the impact on users who are not part of the project and reduces administrative effort by enabling you to apply policies only to the relevant group of users. Once the security group is created, you can then proceed to create an insider risk management policy in the Microsoft Purview portal that targets this group.

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 11 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 11

Topic #: 3

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription. The subscription contains 500 devices that are onboarded to Microsoft Purview.

You select Activate Microsoft Purview Audit.

You need to ensure that you can track interactions between users and generative AI websites.

What should you deploy to the devices?

A. the Microsoft Purview extension **Most Voted**

B. the Microsoft Purview Information Protection client

C. the Microsoft Defender Browser Protection extension

D. Endpoint analytics

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (73%) C (27%)

by dache at *June 8, 2025, 2:12 a.m.*

Comments

58d4802 **Highly Voted** 6 months ago

Selected Answer: A

the Microsoft Purview extension: This is the correct answer. The Microsoft Purview browser extension (for Edge, Chrome, and Firefox on Windows) is specifically designed to provide visibility into user activities on third-party generative AI sites. It's required for Purview's Insider Risk Management and Endpoint DLP to detect visits to these sites and to enforce policies when sensitive information is shared. It enables the auditing of prompts and responses to these AI services.
the Microsoft Defender Browser Protection extension: This extension primarily focuses on protecting users from phishing, malware, and malicious websites by checking URLs against known bad lists. While it's a security tool, its core function is not to track specific user interactions with generative AI sites for Purview auditing purposes.

upvoted 7 times

Lapiduse **Most Recent** 2 months ago

Selected Answer: A

Required for monitoring interactions with third-party generative AI sites:

1. Devices are onboarded to Microsoft Purview, required for:
- Gaining visibility into sensitive information that's shared with third-party generative AI sites.
- Applying endpoint DLP policies to warn or block users from sharing sensitive information with third-party generative AI sites. For example, a user identified as elevated risk in Adaptive Protection is blocked with the option to override when they paste credit card numbers into ChatGPT.

2. The Microsoft Purview browser extension is deployed to Windows users and required to discover visits to third-party generative AI sites by using an Insider Risk Management policy. The browser extension is also required for endpoint DLP policies on Windows when you use Chrome.

https://learn.microsoft.com/en-us/purview/dspm-for-ai-considerations#prerequisites-for-data-security-posture-management-for-ai

upvoted 1 times

Eltooth 2 months, 3 weeks ago

Selected Answer: A

A is correct answer.

upvoted 1 times

Eltooth 2 months, 3 weeks ago

Correction - C. Browser extension.
https://learn.microsoft.com/en-us/purview/dspm-for-ai-considerations#prerequisites-for-data-security-posture-management-for-ai

upvoted 2 times

Jdr379 5 months, 2 weeks ago

Selected Answer: A

The definitive answer is A. the Microsoft Purview extension. This is specifically designed and required for tracking interactions between users and generative AI websites within the Microsoft Purview compliance framework. The Microsoft Defender Browser Protection extension serves a different security purpose and is not the correct tool for this specific requirement.

upvoted 2 times

dache 6 months, 1 week ago

Selected Answer: C

Copilot: To track interactions between users and generative AI websites, the best option is Microsoft Purview Data Security Posture Management for AI (DSPM for AI). This solution provides visibility into AI-related risks, including data oversharing, policy violations, and sensitive information exposure.
However, if you need to deploy a specific tool to devices, Microsoft Defender Browser Protection extension (Option C) is a strong choice for monitoring web activity and enforcing security policies. It helps track user interactions with AI applications and ensures compliance.
https://www.microsoft.com/en-us/security/blog/2025/01/27/fast-track-generative-ai-security-with-microsoft-purview/

upvoted 4 times

PsiCzar 6 months ago

I disagree, DSPM for AI and IRM can track generative AI usage and they require the Purview extension.

According to https://chromewebstore.google.com/detail/microsoft-defender-browse/bkbeeeffjjeopflfhgeknacdieedcoml this is the blurb for the Microsoft Defender Browser Protection extension, which doesnt meet the requirements of the question.

"helps protect you against online threats, such as links in phishing emails and websites designed to trick you into downloading and installing malicious software that can harm your computer. "

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 12 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 12

Topic #: 3

[All SC-401 Questions]

HOTSPOT -

You have a Microsoft 365 subscription.

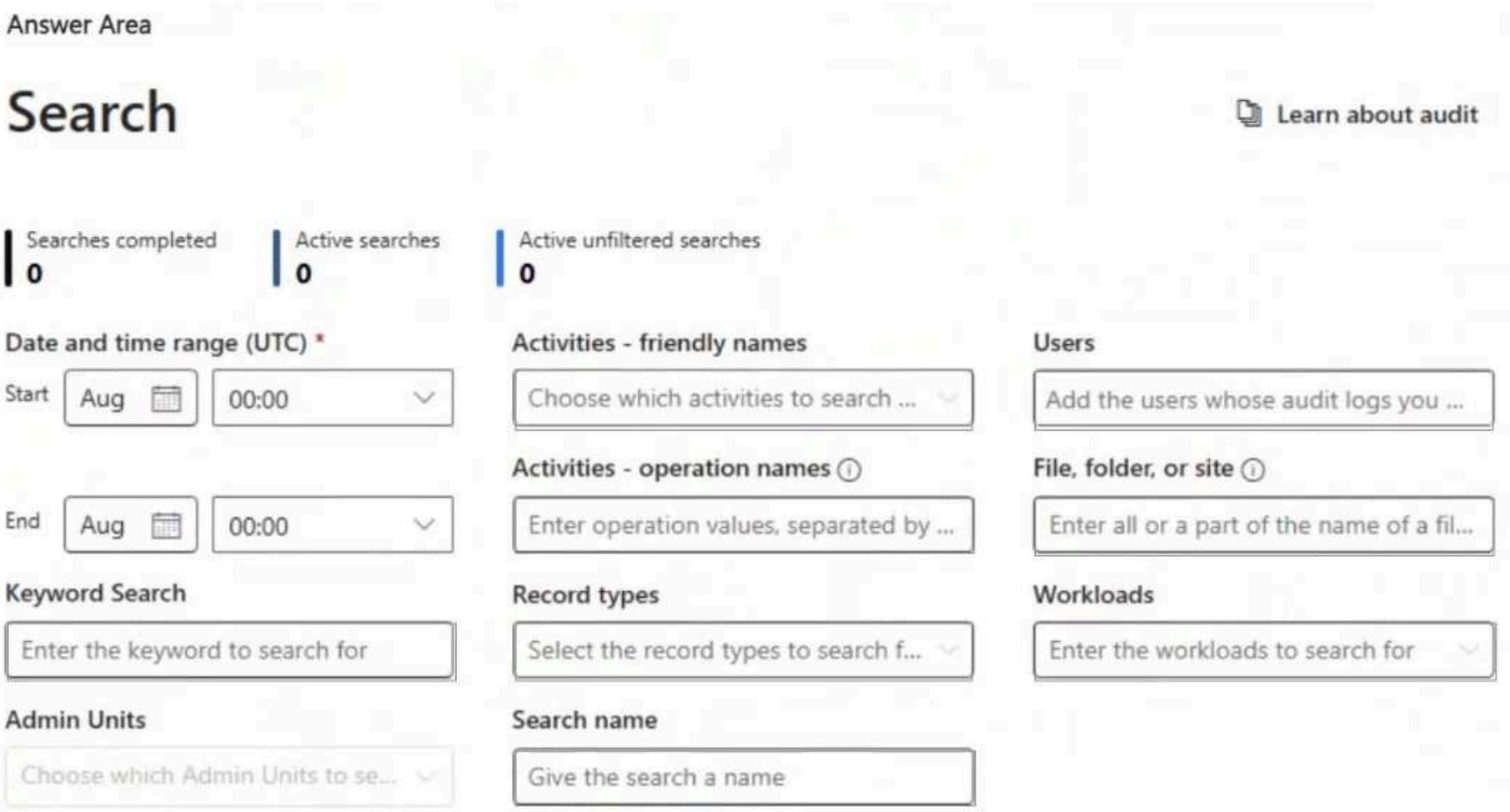
You plan to deploy an audit log retention policy.

You need to perform a search to validate whether the policy will be applied to the intended entries.

Which two fields should you configure for the search? To answer, select the appropriate fields in the answer area.

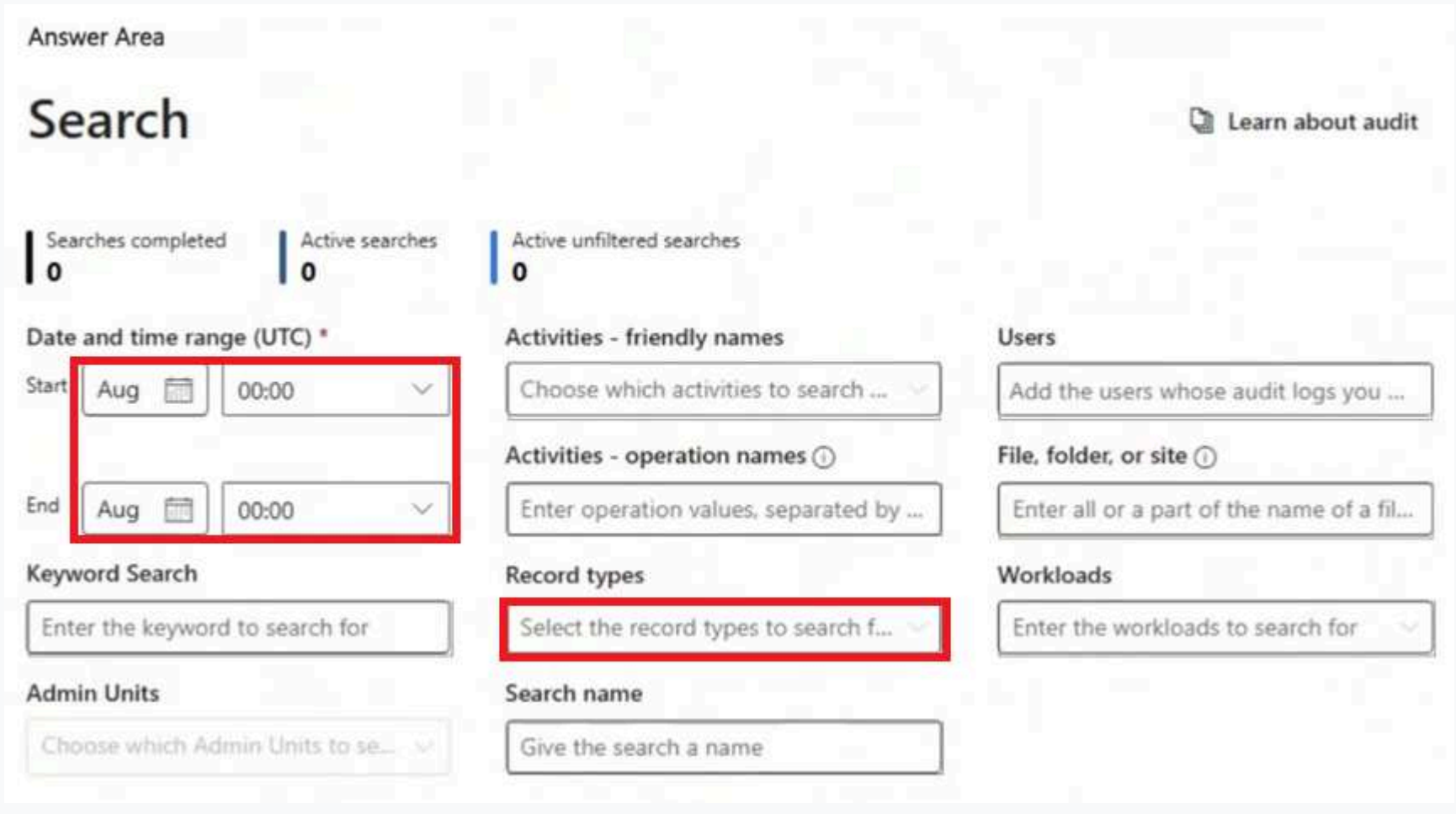
NOTE: Each correct selection is worth one point.

Answer Area



Hide Answer

Suggested Answer:



by Koenst at *June 27, 2025, 8:48 a.m.*

Comments

Koenst Highly Voted 5 months, 2 weeks ago

The answer is not correct. This question was on the exam 25-06-25 but i was not able to select the date and time range.

upvoted 7 times

Eltooth Most Recent 2 months, 3 weeks ago

Users
Record types

upvoted 1 times

gabbinu 3 months, 3 weeks ago

Correct answer: Record types and Users
To validate an audit log retention policy, you can search the Audit search log by using the same record types and users defined in the retention policy.

upvoted 3 times

Jdr379 5 months, 2 weeks ago

https://learn.microsoft.com/en-us/purview/audit-log-retention-policies

1. Record Types
The documentation states: "Record Type: Identify the record type the policy applies to" and "If you select a single record type, the Activities field is dynamically displayed. You can use the drop-down list to select activities from the selected record type to apply the policy to."
2. Workloads
The documentation specifically mentions: "This default policy retains audit records that contain the value of AzureActiveDirectory, Exchange, OneDrive, and SharePoint for the Workload property (which is the service in which the activity occurred). Specific workloads and record types can be changed to a different duration using a retention policy."

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 13 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 13

Topic #: 3

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that uses Microsoft Purview.

You create a communication compliance policy named Policy1 and select Detect Microsoft Copilot interactions.

Which two trainable classifiers will be added to Policy1 automatically? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Unauthorized disclosure

B. Prompt Shields **Most Voted**

C. Threat

D. Corporate Sabotage

E. Protected Materials **Most Voted**

Hide Answer

Suggested Answer: *BE*

Community vote distribution

BE (79%) 14% 7%

by jeff1988 at *May 24, 2025, 11:35 a.m.*

Comments

jeff1988 **Highly Voted** 6 months, 3 weeks ago

Selected Answer: BE

B. Prompt Shields: This classifier is designed to detect unsafe, sensitive, or inappropriate prompts given to generative AI tools like Microsoft Copilot.

E. Protected Materials: This classifier detects when users attempt to expose or use sensitive, confidential, or protected corporate data within Copilot or other generative AI interactions.

upvoted 8 times

Eltooth **Most Recent** 2 months, 3 weeks ago

Selected Answer: BE

Agreed - B & E
Prompt shields
Protected Materials

upvoted 1 times

ZZIN 3 months, 1 week ago

Selected Answer: AB

Microsoft の公式ドキュメントでは、Copilot 関連の Communication Compliance ポリシーを作成したときに 既定で追加されるトレーニング可能な分類子は 2 つとされています。

Prompt Shields (プロンプトシールド)

Unauthorized Disclosure (不正開示)

upvoted 2 times

ppolychron 4 months, 1 week ago

Selected Answer: BE

Conditions: Prompt Shields, Protected material classifiers

https://learn.microsoft.com/en-us/purview/communication-compliance-policies#policy-templates

upvoted 2 times

howter 5 months, 2 weeks ago

Selected Answer: DE

correct

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 14 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 14

Topic #: 3

[All SC-401 Questions]

Your company has offices in multiple countries.

The company has a Microsoft 365 E5 subscription that uses Microsoft Purview insider risk management.

You plan to perform the following actions:

In a new country, open an office named Office1.

Create a new user named User1.

Deploy insider risk management to Office1.

Add User1 to the Insider Risk Management Admins role group.

You need to ensure that User1 can perform insider risk management tasks for only the users and the devices in Office1.

What should you create first?

A. a dynamic device group

B. a dynamic user group

C. an administrative unit **Most Voted**

D. a management group

Hide Answer

Suggested Answer: *C*

Community vote distribution

C (100%)

by Jdr379 at *July 1, 2025, 9:08 p.m.*

Comments

Eltooth 2 months, 3 weeks ago

Selected Answer: C

C is correct answer : Admin unit.

This locks down admin rights to Entra injects within “Office 1” logical boundary

upvoted 2 times

Jdr379 5 months, 2 weeks ago

Selected Answer: C

Answer C

Why Other Options Are Incorrect:
A. Dynamic device group: Device groups don't provide the comprehensive scoping needed for insider risk management across both users and devices
B. Dynamic user group: User groups alone don't provide the administrative scoping mechanism needed
D. Management group: This is an Azure resource management concept, not related to Microsoft Purview insider risk management scoping

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 15 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 15

Topic #: 3

[All SC-401 Questions]

HOTSPOT -

You have a Microsoft 365 E5 subscription.

You need to implement a compliance solution that meets the following requirements:

Captures clips of key security-related user activities, such as the exfiltration of sensitive company data.

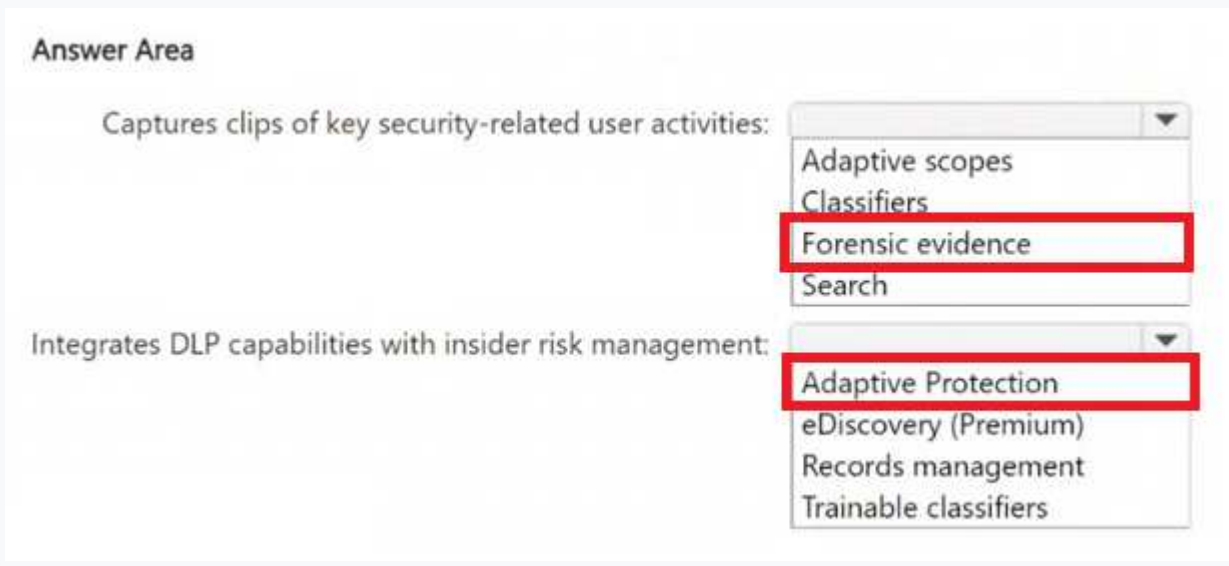
Integrates data loss prevention (DLP) capabilities with insider risk management.

What should you use for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hide Answer

Suggested Answer:



by gabbinu at *Aug. 22, 2025, 10:14 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

Forensic evidence
Adaptive Protection

upvoted 2 times

gabbinu 3 months, 3 weeks ago

Correct answer: Forensic evidence, Adaptive Protection

In Microsoft Purview Insider Risk Management, Forensic evidence allows capturing short screen recordings (clips) of risky user activity, such as data exfiltration attempts.

Adaptive Protection integrates Microsoft Purview DLP with Insider Risk signals.
Users flagged as risky in Insider Risk can automatically be assigned stricter DLP controls.
It ensures DLP dynamically adapts based on insider risk scoring.

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 16 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 16

Topic #: 3

[All SC-401 Questions]

You have a Microsoft 365 subscription.

Users have devices that run Windows 11.

You plan to create a Microsoft Purview insider risk management policy that will detect when a user performs the following actions:

Deletes files that contain a sensitive information type (SIT) from their device

Copies files that contain a SIT to a USB drive

Prints files that contain a SIT -

You need to prepare the environment to support the policy.

What should you do?

A. Configure the physical badging connector.

B. Configure the HR data connector.

C. Create a Microsoft Purview communication compliance policy.

D. Onboard the devices to Microsoft Purview. **Most Voted**

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (100%)

by Jdr379 at *July 1, 2025, 9:14 p.m.*

Comments

Eltooth 2 months, 3 weeks ago

Selected Answer: D

D is correct answer. Onboard device to Purview

upvoted 3 times

Jdr379 5 months, 2 weeks ago

Selected Answer: D

Agree that it's "Onboard the devices to Microsoft Purview"

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 17 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 17

Topic #: 3

[All SC-401 Questions]

HOTSPOT -

You have a Microsoft 365 E5 subscription that contains a user named User1.

You deploy Microsoft Purview Data Security Posture Management for AI (DSPM for AI).

You need to ensure that User1 can perform the following actions:

View recommendations from the Recommendations page.

View the user risk level for all events by using Activity explorer.

The solution must follow the principle of least privilege.

To which role group should you add User1 for each action? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

View the recommendations:

- Compliance Administrator
- Insider Risk Management Investigators
- Security Reader

View the user risk level:

- Compliance Administrator
- Insider Risk Management Analysts
- Insider Risk Management Investigators
- Security Reader

Hide Answer

Suggested Answer:

by papillor at *June 6, 2025, 12:59 p.m.*

Comments

CuentaRM10 Highly Voted 6 months ago

It should be Security Reader and IRM Analyst
https://learn.microsoft.com/en-us/purview/ai-microsoft-purview-permissions

upvoted 12 times

gabbinu Highly Voted 3 months, 3 weeks ago

View all recommendations -> Microsoft Purview Security Reader role group
View user risk level in Activity Explorer -> Insider Risk Management Analyst

upvoted 5 times

Eltooth Most Recent 2 months, 3 weeks ago

Security Reader
Insider Risk Management Analyst

upvoted 2 times

papillor 6 months, 1 week ago

Wrong.
Answer 1 = Security Reader - DSPM for AI has nothing to do with IRM
Answer 2 : Insider Risk Management Investigators. Analysts role doesn't give enough permission to access user risk level.

upvoted 2 times

PsiCzar 6 months, 1 week ago

According to Permissions by Activities on this page, its Security Reader and Microsoft Purview Insider Risk Management Analyst.
https://learn.microsoft.com/en-us/purview/ai-microsoft-purview-permissions

upvoted 5 times

dache 6 months, 1 week ago

Coiplot: Based on the image details and Microsoft Purview documentation, here are the correct role groups for User1:
- View recommendations from the Recommendations page: Security Reader
- View the user risk level for all events using Activity Explorer: Insider Risk Management Analysts
These selections ensure User1 has the least privilege necessary to perform the required actions while maintaining security and compliance.
https://learn.microsoft.com/en-us/purview/ai-microsoft-purview-permissions

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 18 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 18

Topic #: 3

[All SC-401 Questions]

HOTSPOT -

You have a Microsoft 365 E5 subscription that uses Microsoft Purview.

You need ensure that an incident will be generated when a user visits a phishing website.

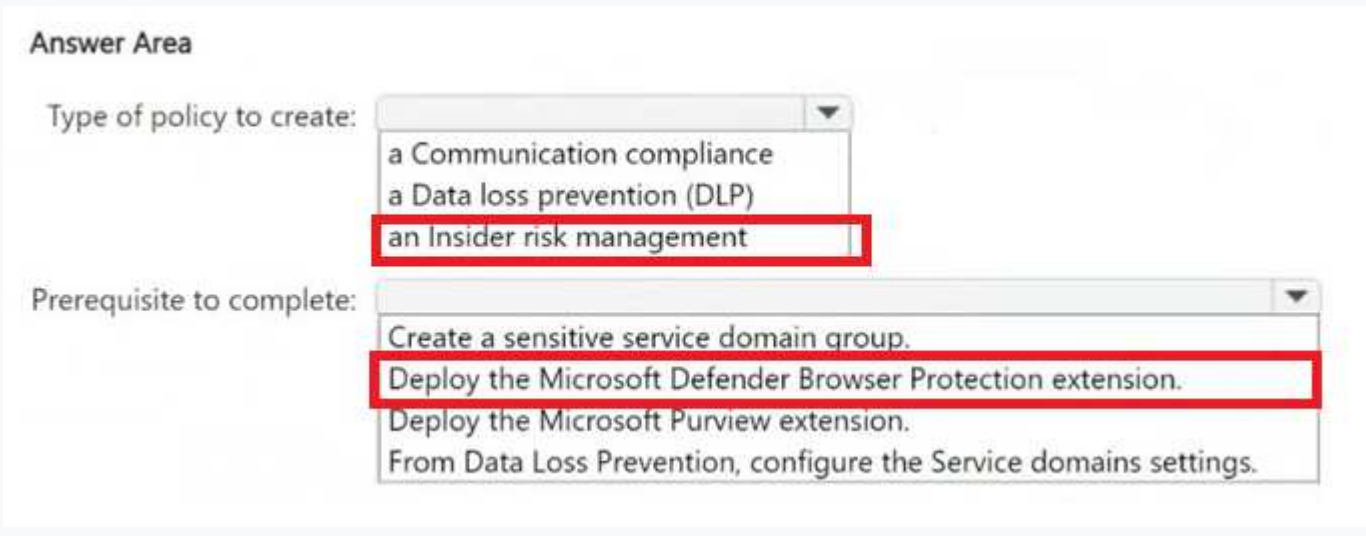
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area
Type of policy to create:
a Communication compliance
a Data loss prevention (DLP)
an Insider risk management
Prerequisite to complete:
Create a sensitive service domain group.
Deploy the Microsoft Defender Browser Protection extension.
Deploy the Microsoft Purview extension.
From Data Loss Prevention, configure the Service domains settings.

Hide Answer

Suggested Answer:


Answer Area
Type of policy to create:
a Communication compliance
a Data loss prevention (DLP)
an Insider risk management
Prerequisite to complete:
Create a sensitive service domain group.
Deploy the Microsoft Defender Browser Protection extension.
Deploy the Microsoft Purview extension.
From Data Loss Prevention, configure the Service domains settings.

by PsiCzar at *June 9, 2025, 6:56 a.m.*

Comments

PsiCzar Highly Voted 6 months, 1 week ago

Incorrect, it should be Insider Risk Management and Microsoft Purview extension. Confirmed in my dev environment. Deploying an IRM Risky browser usage policy has a prerequisite for the Purview extension to be installed. Inside the policy you can select a triggering event of Browsed to phishing websites.

upvoted 10 times

Eltooth Most Recent 2 months, 3 weeks ago

Risky browser usage (preview)
Prerequisites:
IRM
Purview extension
At least one browsing indicator selected

Also confirmed in my tenant.

upvoted 2 times

deeptha92 3 months, 2 weeks ago

Insider Risk Management
Microsoft Purview Extension

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 19 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 19

Topic #: 3

[All SC-401 Questions]

You have Microsoft 365 E5 subscription.

You create two alert policies named Policy1 and Policy2 that will be triggered at the times shown in the following table.

Policy	Time (hh:mm:ss)
Policy1	10:00:00
Policy2	10:00:03
Policy1	10:00:04
Policy2	10:00:31
Policy1	10:01:01
Policy1	10:04:45

How many alerts will be added to the Microsoft Purview portal?

A. 2

B. 3

C. 4 **Most Voted**

D. 5

E. 6

Hide Answer

Suggested Answer: *C*

Community vote distribution

C (81%) Other

by jeff1988 at *May 24, 2025, 11:43 a.m.*

Comments

PsiCzar **Highly Voted** 6 months, 1 week ago

Selected Answer: C

Answer is incorrect, it should be C. 4, based on https://learn.microsoft.com/en-us/purview/compliance-manager-alert-policies

"When multiple events that match the conditions of an alert policy occur within one minute, they're added to an existing alert by a process called alert aggregation." So:
Policy 1: has 3 alerts in less than a minute, so 1 alert is generated, then a further 2 alerts separated by more than a minute each, consolidated that's 3 alerts
Policy 2: has 2 alerts all within the same minute, so that is 1 alert

upvoted 11 times

Jdr379 5 months, 2 weeks ago

I concur that it's C.

upvoted 2 times

brugmany Most Recent 3 weeks, 6 days ago

Selected Answer: C

In Purview, if several events trigger the same alert policy within one minute, they are grouped into a single alert instead of creating separate ones.

Policy1 at 10:00:00 & 10:00:04 = 1 alert
Policy1 at 10:01:01 = 2nd alert
Policy1 at 10:04:45 = 3rd alert
Policy2 at 10:00:03 & 10:00:31 = 1 alert

https://learn.microsoft.com/en-us/purview/compliance-manager-alert-policies

upvoted 1 times

Eltooth 2 months, 3 weeks ago

Selected Answer: C

C is correct answer.
https://learn.microsoft.com/en-us/purview/compliance-manager-alert-policies#alert-aggregation-for-multiple-events-within-one-minute

upvoted 1 times

Eltooth 2 months, 3 weeks ago

"When multiple events that match the conditions of an alert policy occur with one minute, they're added to an existing alert by a process called alert aggregation.

For example, when one event occurs which matches a policy, an alert is generated and displayed on the Alerts page and a notification is sent. If another event matching the same policy occurs within one minute of the first event, then Compliance Manager adds details about the other event on the Events log tab of the existing alert instead of triggering a new alert. The goal of alert aggregation is to help reduce alert "fatigue" and let you focus and take action on fewer alerts."

upvoted 1 times

Jdr379 5 months, 2 weeks ago

Selected Answer: C

Answer is C.

Microsoft 365 E5: 1-minute aggregation interval

Same aggregation logic: When multiple events that match the conditions of an alert policy occur with a short period of time, they're added to an existing alert by a process called alert aggregation

upvoted 4 times

4d76265 6 months ago

Selected Answer: C

PsiCzar's answer is the best here with MS reference.

upvoted 2 times

CuentaRM10 6 months ago

Selected Answer: C

Sorry, it should be C
To prevent alert overload, policy matches on the same item in the same location are grouped if they occur within a one-minute window.

https://learn.microsoft.com/en-us/training/modules/purview-data-loss-prevention-alerts/configure-data-loss-prevention-alert-generation

upvoted 2 times

CuentaRM10 6 months ago

Selected Answer: A

It should be Answer A.
All matches that are detected within a span of 60 minutes will be grouped into one single alert to reduce excessive notifications

https://learn.microsoft.com/en-us/purview/compliance-manager-alert-policies#default-score-change-policy

upvoted 1 times

papillor 6 months, 1 week ago

Selected Answer: A

Correction Good answer is A !! Only 2 alerts ! I misclicked.

upvoted 1 times

papillor 6 months, 1 week ago

Selected Answer: B

When the same alert is generated multiple times within a short period (by default 5 minutes), Microsoft Purview consolidates these occurrences into a single alert in the portal.

upvoted 1 times

jeff1988 6 months, 3 weeks ago

Selected Answer: E

Each alert policy triggers independently based on the specified times. Here are the times again:

Policy1: 10:00:00, 10:00:04, 10:01:01, 10:04:45 (4 alerts)
Policy2: 10:00:03, 10:00:31 (2 alerts)
Since each trigger time results in a separate alert, we count all the times:

Policy1: 4 alerts
Policy2: 2 alerts
Adding them together, we get 6 alerts. Therefore, the correct answer is E. 6.

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 20 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 20

Topic #: 3

[All SC-401 Questions]

HOTSPOT -

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role group
Admin1	Insider Risk Management Admins
Admin2	Insider Risk Management Analysts
Admin3	Risk Management Investigators
Admin4	Insider Risk Management Auditors

You plan to create a Microsoft Purview insider risk management case named Case1.

Which insider risk management object should you select first, and which users will be added as contributors for Case1 by default?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

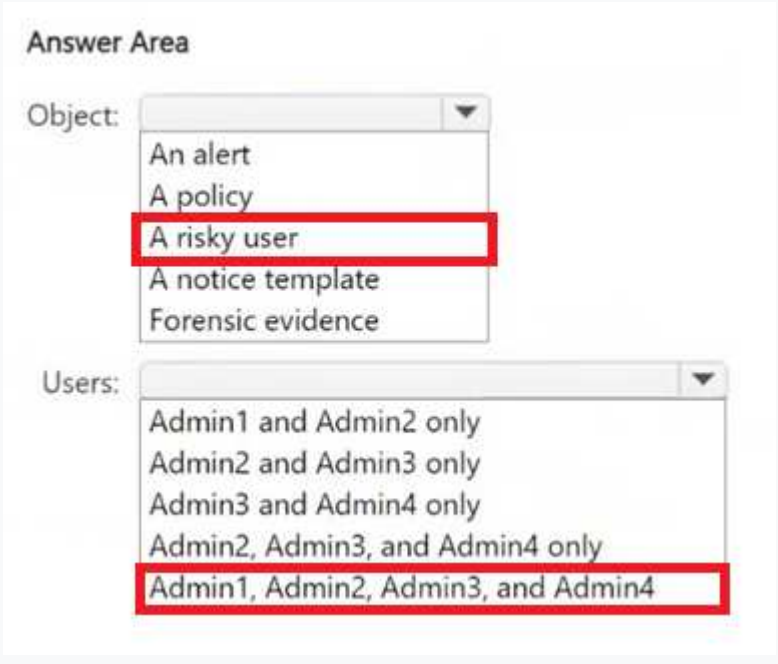
Answer Area

Object:
- An alert
- A policy
- A risky user
- A notice template
- Forensic evidence

Users:
- Admin1 and Admin2 only
- Admin2 and Admin3 only
- Admin3 and Admin4 only
- Admin2, Admin3, and Admin4 only
- Admin1, Admin2, Admin3, and Admin4

Hide Answer

Suggested Answer:



by PsiCzar at *June 9, 2025, 7:50 a.m.*

Comments

Alcpt 1 week, 6 days ago

This is an ambiguous scenario question:
In the typical flow for creating a case inside the portal, you go to Insider risk management > Cases > + New case. Then you must choose either:
A risky user (to start from scratch), or
An alert (to start from an existing triggered alert).

Since the question doesn't mention that you already have pre-existing alerts or that you're manually creating a case for a user without alerts, one might think both are possible. But for exam purposes, I would think the expected Microsoft answer is usually "An alert" because of the slant towards automation.
Geez, its a 50/50 here in my opinion.

Users: Admin2 and Admin 3 are created by default.

upvoted 1 times

Caezarlay 2 months, 2 weeks ago

Object: An alert
Users: Admin2 and Admin 3

upvoted 3 times

Eltooth 2 months, 3 weeks ago

A policy should be created first - how is an alert going to be generated without?
Default access is Admin 2 & admin 3 (Insider Risk Management Analysts & Insider Risk Management Investigators)

upvoted 2 times

gabbinu 3 months, 3 weeks ago

Object: An alert
When you create a case in Microsoft Purview Insider Risk Management, you always start from an alert.
Cases are used to investigate alerts in more detail.

Users:Admin1, Admin2, Admin3, and Admin4
By default, all users assigned the Insider Risk Management Investigators and the Insider Risk Management roles are listed as contributors for each active and closed case.
https://learn.microsoft.com/en-us/purview/insider-risk-management-cases

upvoted 3 times

examtopicssc401 6 months ago

Correct: An alert

To create a case in Microsoft Purview insider risk management, you always start from an alert.

Which users are added as contributors by default?

Insider Risk Management

Admin3 (Insider Risk Management Investigators)

Cab access

Admin2 (Insider Risk Management Analysts)

NO rights

Admin1 (Insider Risk Management Admin)

Admin4 (Insider Risk Management Auditors)
https://learn.microsoft.com/en-us/purview/insider-risk-management-configure#step-1-required-enable-permissions-for-insider-risk-management

upvoted 1 times

CuentaRM10 6 months, 1 week ago

Object it's correct: Risky User
But the users should be Admin1, Admin2 and Admin3 since Insider risk management auditors have not necesary permissions to view case reports
https://learn.microsoft.com/en-us/purview/insider-risk-management-configure#step-1-required-enable-permissions-for-insider-risk-management

upvoted 1 times

PsiCzar 6 months, 1 week ago

Appears to be correct.

The first part is probably correct based on https://learn.microsoft.com/en-us/purview/insider-risk-management-activities which says "Investigating potentially risky user activities is an important first step in minimizing insider risks for your organization."

The second part is correct based on https://learn.microsoft.com/en-us/purview/insider-risk-management-cases which says "By default, all users assigned the Insider Risk Management Investigators and the Insider Risk Management roles are listed as contributors for each active and closed case."

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 21 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 21

Topic #: 3

[All SC-401 Questions]

HOTSPOT -

You have a Microsoft 365 E5 subscription that uses Microsoft Purview and just-in-time (JIT) protection. The subscription contains the users shown in the following table.

Name	JIT protection scope
User1	Included
User2	Not configured
User3	Included

The subscription contains the devices shown in the following table.

Name	Microsoft Defender
Device1	Onboarded
Device2	Onboarded
Device3	Not onboarded

The devices contain the files shown in the following table.

Name	File classification evaluation status	Location
File1.docx	Not evaluated	Device1
File2.pdf	Evaluated	Device2
File3.xlsx	Not evaluated	Device3

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If User1 attempts to copy File1.docx to a removable USB drive, JIT will block the action.	○	○
If User2 signs in to Device2 and attempts to attach File2.pdf to an email, JIT will block the action.	○	○
If User3 attempts to copy File3.xlsx to a network share, JIT will generate an audit event.	○	○

Hide Answer

Suggested Answer:

Answer Area

Statements	Yes	No
If User1 attempts to copy File1.docx to a removable USB drive, JIT will block the action.	○	●
If User2 signs in to Device2 and attempts to attach File2.pdf to an email, JIT will block the action.	○	●
If User3 attempts to copy File3.xlsx to a network share, JIT will generate an audit event.	○	●

by SH_Train at *June 5, 2025, 4:34 a.m.*

Comments

SH_Train Highly Voted 6 months, 1 week ago

User1 is in scope for JIT and the device is onboarded. The file is not evaluated thus will be blocked until evaluation is complete. Answer should be Yes.

upvoted 10 times

Caezarlay Most Recent 2 months, 2 weeks ago

Yes
No
No

upvoted 2 times

Eltooth 2 months, 3 weeks ago

Yes
No
No

upvoted 1 times

RickySmith 2 months, 3 weeks ago

Yes
No
No
User1 is in scope for JIT and the device is onboarded. The file is not evaluated thus will be blocked until evaluation is complete. Answer should be Yes.
https://learn.microsoft.com/en-us/purview/endpoint-dlp-get-started-jit
When JIT protection is enabled, and while policy evaluation is processing, Endpoint DLP blocks all egress activities for each user whose account is in the selected scope.

upvoted 2 times

Jdr379 5 months, 2 weeks ago

I believe it should be
Yes
No
No
Reasoning:
Statement 1 Breakdown:
User1: In JIT scope ✅
Device1: Onboarded
File1.docx: "Not evaluated" - this is the KEY trigger for JIT protection
Action: Copy to USB (egress activity) ✅

How JIT Should Work:
User1 attempts to copy File1.docx to USB
JIT sees the file is "not evaluated"
JIT immediately blocks the egress activity
Classification/evaluation begins in the background
Once evaluation completes, appropriate DLP policy actions apply

JIT protection is specifically designed to block BEFORE evaluation completes, regardless of what the final policy determination will be.

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 22 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 22

Topic #: 3

[All SC-401 Questions]

You need to be alerted when users share sensitive documents from Microsoft OneDrive to any users outside your company.

What should you do?

A. From the Microsoft Purview portal, create an insider risk policy.

B. From the Microsoft Defender portal, create a file policy. **Most Voted**

C. From the Microsoft Defender portal, create an activity policy.

D. From the Microsoft Purview portal, start a data investigation.

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (67%) A (20%) 13%

by PsiCzar at *June 12, 2025, 8 a.m.*

Comments

Koenst Highly Voted 5 months, 3 weeks ago

Selected Answer: B

I think a file policy is the better answer

upvoted 5 times

Eltooth Most Recent 2 months, 3 weeks ago

Selected Answer: B

B is correct answer - File policy.

upvoted 1 times

Gtc_ 3 months, 2 weeks ago

Selected Answer: B

It's in the docs

https://learn.microsoft.com/en-us/defender-cloud-apps/control-cloud-apps-with-policies

upvoted 2 times

gabbinu 3 months, 3 weeks ago

Selected Answer: B

Correct answer should be B
https://learn.microsoft.com/en-us/defender-cloud-apps/data-protection-policies
The following are examples of file policies that can be created:
Sharing with external domains - Receive an alert about any file shared with accounts owned by specific external domains.

upvoted 2 times

ppolychron 4 months, 1 week ago

Selected Answer: A

What is considered "sensitive" for the organization? Is it documents with specific Sensitivity Label or a Specific SIT?

I think the tool that gives you the flexibility to handle whatever is considered sensitive, is a Insider Risk Management Policy with a DLP Policy as Trigger and priority content if needed on top.

upvoted 1 times

Jdr379 5 months, 2 weeks ago

Selected Answer: A

I think with the updated features, the answer is A.

Defender for Cloud Apps = Monitors third-party cloud apps (Box, Dropbox, Google Drive)
Insider Risk Management = Monitors internal user risks within Microsoft 365 (OneDrive, SharePoint, Teams)

The Question Scenario:

WHO: Internal employees
WHAT: Sharing sensitive documents externally
WHERE: From OneDrive (Microsoft 365 service)
CLASSIFICATION: This is an "insider risk" - internal users potentially violating policy

Simple Rule:

Microsoft 365 services (OneDrive, SharePoint) → Insider Risk Management
Third-party cloud apps → Defender for Cloud Apps

This represents Microsoft's shift toward "Purview-first" for internal compliance scenarios, even though both solutions technically work.
https://learn.microsoft.com/en-us/purview/insider-risk-management-settings-policy-indicators

upvoted 2 times

PsiCzar 6 months ago

Selected Answer: C

Correct. An Activity policy can track and alert on sharing activities from SP/OD.

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 23 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 23

Topic #: 3

[All SC-401 Questions]

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You have a user named User1. Several users have full access to the mailbox of User1.
Some email messages sent to User1 appear to have been read and deleted before the user viewed them.
When you search the audit log in the Microsoft Purview portal to identify who signed in to the mailbox of User1, the results are blank.
You need to ensure that you can view future sign-ins to the mailbox of User1.
Solution: You run the Set-MailboxFolderPermission -Identity "User1" -User User1@contoso.com -AccessRights Owner command.
Does that meet the goal?

A. Yes

B. No

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (100%)

by Eltooth at *Sept. 22, 2025, 5:57 p.m.*

Comments

Eltooth 2 months, 3 weeks ago

Selected Answer: B

No
Mailbox auditing must be explicitly enabled for User1 if it hasn't already been.
Also, to track sign-ins by other users with delegated access (e.g., full access), you must ensure that audit logging for delegate access is enabled.
1. Set-Mailbox User1 -AuditEnabled $true
2. Set-Mailbox User1 -AuditDelegate SendOnBehalf, SendAs, Access
3. Verify that Unified Audit Logging is enabled in Microsoft Purview:

Go to Microsoft Purview portal → Audit → Audit settings
Ensure Audit (Standard) or Audit (Premium) is turned on.

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 24 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 24

Topic #: 3

[All SC-401 Questions]

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You have a user named User1. Several users have full access to the mailbox of User1.
Some email messages sent to User1 appear to have been read and deleted before the user viewed them.
When you search the audit log in the Microsoft Purview portal to identify who signed in to the mailbox of User1, the results are blank.
You need to ensure that you can view future sign-ins to the mailbox of User1.
Solution: You run the Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -AdminAuditLogCmdlets *Mailbox* command.
Does that meet the goal?

A. Yes

B. No **Most Voted**

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (100%)

by ETUs3r at *April 4, 2025, 10:37 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

Selected Answer: B

No
Mailbox auditing must be explicitly enabled for User1 if it hasn't already been.
Also, to track sign-ins by other users with delegated access (e.g., full access), you must ensure that audit logging for delegate access is enabled.
1. Set-Mailbox User1 -AuditEnabled $true
2. Set-Mailbox User1 -AuditDelegate SendOnBehalf, SendAs, Access
3. Verify that Unified Audit Logging is enabled in Microsoft Purview:

Go to Microsoft Purview portal → Audit → Audit settings
Ensure Audit (Standard) or Audit (Premium) is turned on.

upvoted 1 times

deeptha92 3 months, 2 weeks ago

Selected Answer: B

That enables admin actions, not user activities in the mailbox, such as deleting an item.

upvoted 1 times

ETUs3r 8 months, 1 week ago

Selected Answer: B

Set-AdminAuditLogConfig cmdlet is to configure the administrator audit logging configuration settings not mailbox audit logging.

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 25 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 25

Topic #: 3

[All SC-401 Questions]

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You have a user named User1. Several users have full access to the mailbox of User1.
Some email messages sent to User1 appear to have been read and deleted before the user viewed them.
When you search the audit log in the Microsoft Purview portal to identify who signed in to the mailbox of User1, the results are blank.
You need to ensure that you can view future sign-ins to the mailbox of User1.
Solution: You run the Set-Mailbox -Identity "User1" -AuditEnabled $true command.
Does that meet the goal?

A. Yes **Most Voted**

B. No

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (100%)

by ETUs3r at *April 4, 2025, 10:27 a.m.*

Comments

gabbinu 3 months, 3 weeks ago

Selected Answer: A

Mailbox auditing is enabled by default for all users.
https://learn.microsoft.com/en-us/purview/audit-mailboxes
However, if auditing was disabled, with this command you can ensure it's explicitly enabled for User1.

upvoted 1 times

Jarem 6 months ago

Selected Answer: A

Yes, this solution meets the goal. Running the Set-Mailbox -Identity "User1" -AuditEnabled $true command enables mailbox auditing for User1's mailbox. This will allow you to track future sign-ins and other activities on User1's mailbox, ensuring you can identify who accessed the mailbox.

upvoted 1 times

ETUs3r 8 months, 1 week ago

Selected Answer: A

When you enable mailbox audit logging for a mailbox, some actions performed by administrators and delegates are logged by default.

https://learn.microsoft.com/en-us/exchange/policy-and-compliance/mailbox-audit-logging/enable-or-disable?view=exchserver-2019
https://learn.microsoft.com/en-us/purview/audit-mailboxes

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 26 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 26

Topic #: 3

[All SC-401 Questions]

Your company has Microsoft 369 E5 subscription and plans to use Microsoft Purview Advanced Message Encryption.

Each product group at your company must show a distinct product logo in encrypted emails instead of the standard Microsoft 365 logo.

What should you do to create the branding templates?

A. Create an RMS template.

B. Create a Transport rule.

C. Run the New-OMEConfiguration cmdlet. **Most Voted**

D. Run the Set-IRMConfiguration cmdlet.

Hide Answer

Suggested Answer: *C*

Community vote distribution

C (100%)

by Kamiles at *Aug. 25, 2025, 3:33 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

Selected Answer: C

C is correct answer.
https://learn.microsoft.com/en-us/powershell/module/exchangepowershell/new-omeconfiguration?view=exchange-ps#-image

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 27 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 27

Topic #: 3

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Role
User1	Compliance Administrator
User2	Security Operator
User3	eDiscovery Manager

You need to implement sensitivity labels.

Which users can create sensitivity labels, and which portal should the users use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

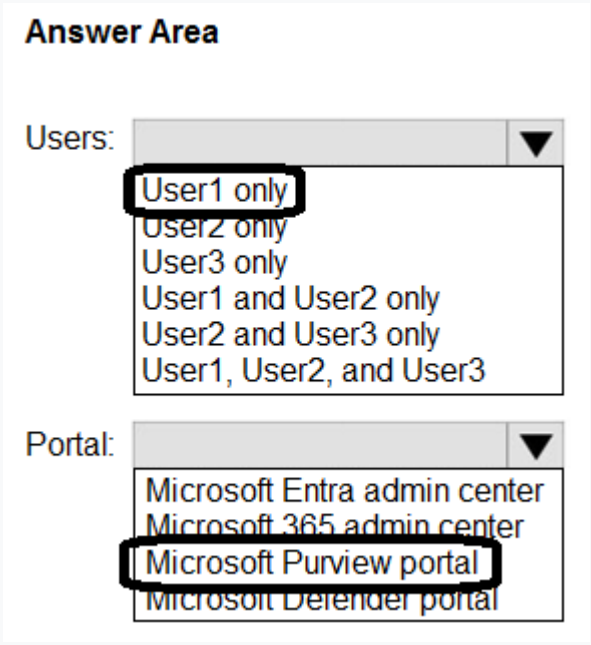
Answer Area

Users:
- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Portal:
- Microsoft Entra admin center
- Microsoft 365 admin center
- Microsoft Purview portal
- Microsoft Defender portal

Hide Answer

Suggested Answer:



by Seidor_Analytics at *Sept. 5, 2025, 8:24 a.m.*

Comments

Eltooth Highly Voted 2 months, 3 weeks ago

User 1 only
Purview

upvoted 5 times

RickySmith Most Recent 2 months, 3 weeks ago

1,3
https://learn.microsoft.com/en-us/purview/get-started-with-sensitivity-labels#permissions-required-to-create-and-manage-sensitivity-labels

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 28 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 28

Topic #: 3

[All SC-401 Questions]

HOTSPOT

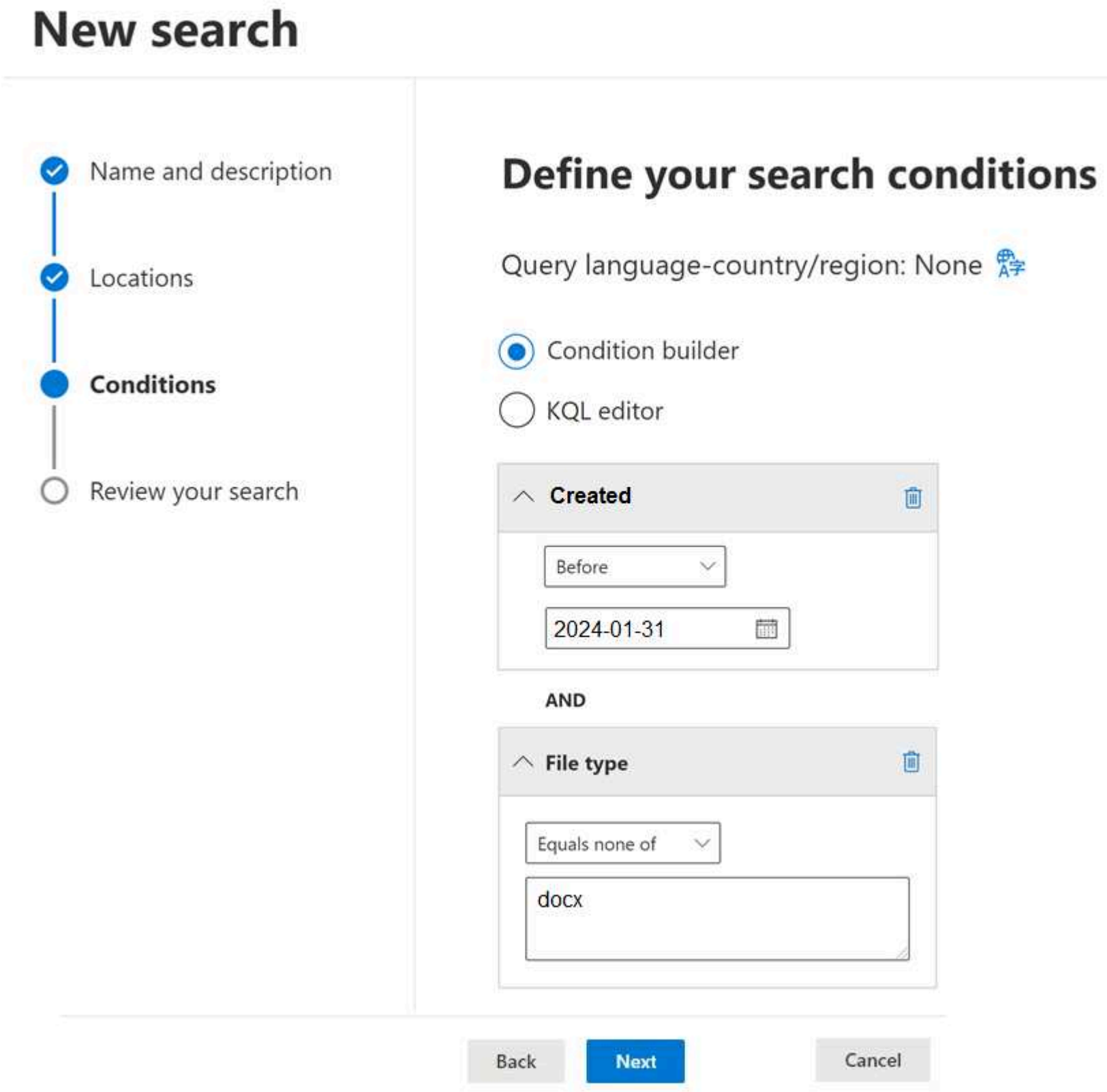
-

You have a Microsoft 365 subscription.

You have a Microsoft SharePoint Online site named Site1. Site1 has a document library that contains the files shown in the following table.

Name	File type	Created on
File1	DOCX	December 1, 2023
File2	XLSX	February 5, 2024
File3	PNG	May 4, 2023

From the Microsoft Purview compliance portal, for Site1 you create a content search named Search1 that has the date in the YYYY-MM-DD format as shown in the following exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
File1 is included in the Search1 results.	○	○
File2 is included in the Search1 results.	○	○
File3 is included in the Search1 results.	○	○

Hide Answer

Suggested Answer:

Answer Area

Statements	Yes	No
File1 is included in the Search1 results.	○	●
File2 is included in the Search1 results.	○	●
File3 is included in the Search1 results.	●	○

by Seidor_Analytics at *Sept. 5, 2025, 8:24 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

Answers are correct.
No
No
Yes

upvoted 3 times

RickySmith 2 months, 3 weeks ago

NNY
Correct

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 29 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 29

Topic #: 3

[All SC-401 Questions]

You have a Microsoft 365 subscription that contains the devices shown in the following table.

Name	Platform	Microsoft Purview	Microsoft Purview client
Device1	Windows 11	Not onboarded	Installed
Device2	Windows 10	Onboarded	Installed
Device3	macOS	Onboarded	Not installed

From which devices can Microsoft Purview Insider Risk Management capture forensic evidence?

A. Device1 only

B. Device2 only **Most Voted**

C. Device1 and Device2 only

D. Device2 and Device3 only

E. Device1, Device2, and Device3

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:25 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

Selected Answer: B

B is correct answer.
"Devices must be onboarded and have the Microsoft Purview client installed: Before forensic evidence can collect and store clips captured for eligible users, their devices must be onboarded to the Microsoft Purview portal. Additionally, each device must have the Microsoft Purview Client installed. These prerequisites enable support for both online and offline device capturing."

https://learn.microsoft.com/en-us/purview/insider-risk-management-forensic-evidence#workflow

upvoted 2 times

RickySmith 2 months, 3 weeks ago

Selected Answer: B

B

https://learn.microsoft.com/en-us/purview/insider-risk-management-forensic-evidence#workflow

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 30 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 30

Topic #: 3

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Microsoft Purview role group	Microsoft 365 role
User1	*None*	Global Administrator
User2	Insider Risk Management Analysts	*None*
User3	Insider Risk Management Investigations	*None*

The subscription contains the groups shown in the following table.

Name	Type
Group1	Security
Group2	Microsoft 365

You plan to create a priority user group named Priority1.

You need to identify the following:

- Which users and groups can be added to Priority1?
- Which users can be enabled to view alerts that involve the members of Priority1?

What should you identify? To answer, select the appropriate options in the answer area.

Answer Area

Can be added to Priority1:

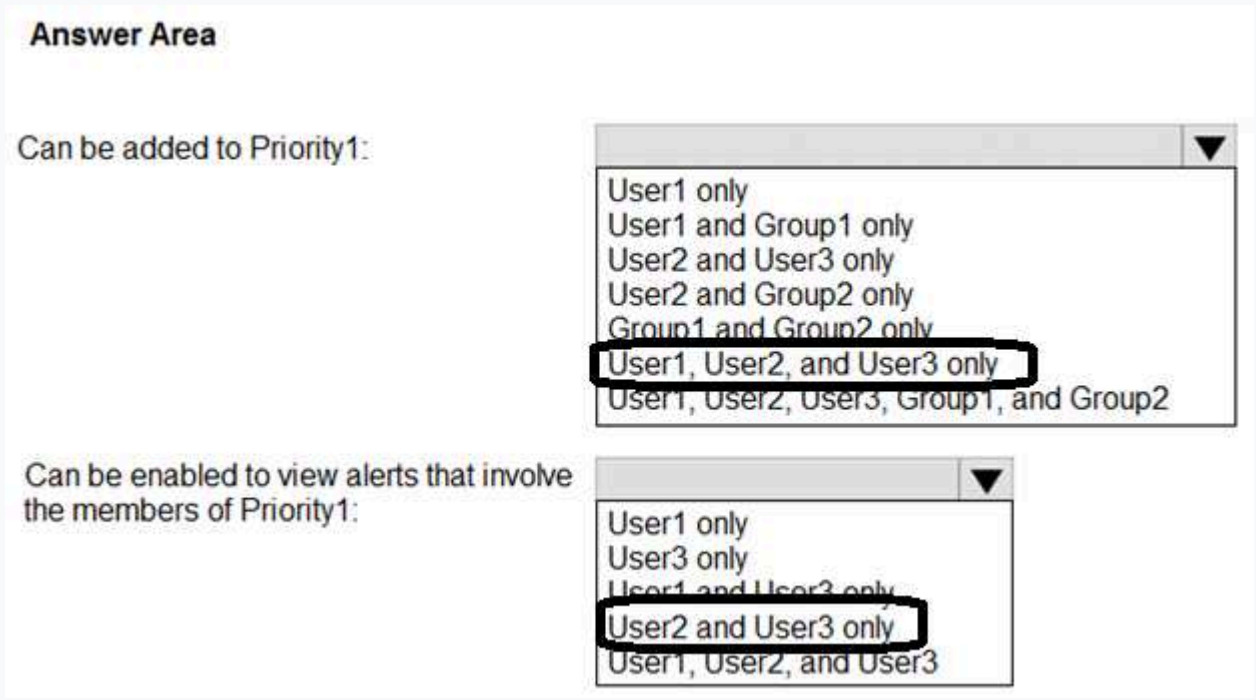
- User1 only
- User1 and Group1 only
- User2 and User3 only
- User2 and Group2 only
- Group1 and Group2 only
- User1, User2, and User3 only
- User1, User2, User3, Group1, and Group2

Can be enabled to view alerts that involve the members of Priority1:

- User1 only
- User3 only
- User1 and User3 only
- User2 and User3 only
- User1, User2, and User3

Hide Answer

Suggested Answer:


Answer Area
Can be added to Priority1:
User1 only
User1 and Group1 only
User2 and User3 only
User2 and Group2 only
Group1 and Group2 only
User1, User2, and User3 only
User1, User2, User3, Group1, and Group2
Can be enabled to view alerts that involve the members of Priority1:
User1 only
User3 only
User1 and User3 only
User2 and User3 only
User1, User2, and User3

by Seidor_Analytics at *Sept. 5, 2025, 8:17 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

User 1, 2 & 3.

"On the Choose members page, select Choose members to search and select which mail-enabled user accounts are included in the group or select the Select all checkbox to add all users in your organization to the group. "

User 2 & 3.
https://learn.microsoft.com/en-us/purview/insider-risk-management-permissions

upvoted 2 times

RickySmith 2 months, 3 weeks ago

User1, User 2 and User 3 only
User 2 and User 3 only
https://learn.microsoft.com/en-us/purview/insider-risk-management-settings-priority-user-groups#create-a-priority-user-group

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 31 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 31

Topic #: 3

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 E5 subscription that uses Microsoft Purview.

You need to deploy a compliance solution that will detect the accidental oversharing of information outside of an organization. The solution must minimize administrative effort.

What should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Policy template:

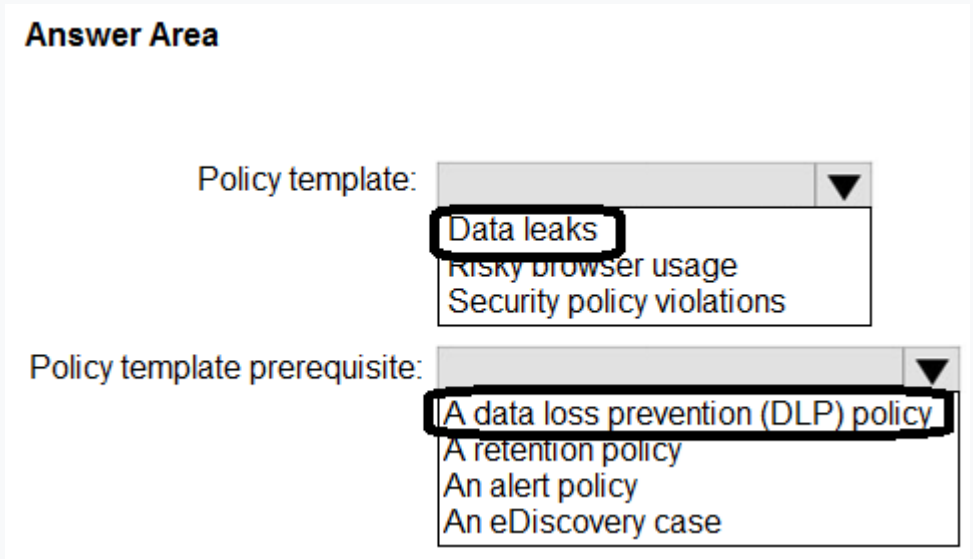
- Data leaks
- Risky browser usage
- Security policy violations

Policy template prerequisite:

- A data loss prevention (DLP) policy
- A retention policy
- An alert policy
- An eDiscovery case

Hide Answer

Suggested Answer:



by Seidor_Analytics at *Sept. 5, 2025, 8:15 a.m.*

Comments

Alcpt 1 week, 6 days ago

given answers are correct:
Technically, you could also set up an alert policy as a trigger. However, in the exam, the default/recommended answer for "data leaks" scenario prerequisites is DLP policy because:
DLP is already monitoring data flows,
Using DLP as a trigger reuses existing configurations which minimizes effort,

Alert policies are more for security alerts (like from Microsoft Defender for Office 365), not primarily for accidental oversharing detection.

upvoted 1 times

RickySmith 2 months, 3 weeks ago

This is a messed up question.
The Policy Template question is from IRM Policies.
The Pre-requisites are from all of Purview.
I am looking at this from selectable answers and the questions itself.

"detect" - meaning alert
"accidental oversharing of information outside of an organization" - data leaks

So
Data Leaks
An alert Policy

upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 32 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 32

Topic #: 3

[All SC-401 Questions]

DRAG DROP

-

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft Purview Insider Risk Management.

You obtain a file named File1.csv that contains employee resignation data.

You need to implement the HR data connector and upload File1.csv by using the connector.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

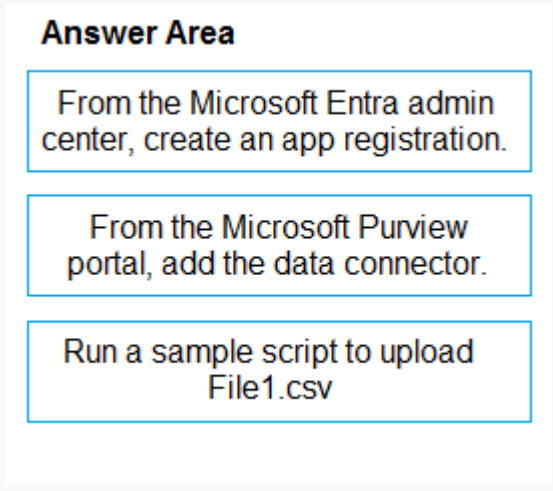
Actions

- Configure the Insider Risk Management settings.
- From the Microsoft Purview portal, add the data connector.
- From the Microsoft Entra admin center, create an app registration.
- Implement Microsoft Entra Connect sync.
- Run a sample script to upload File1.csv

Answer Area

Hide Answer

Suggested Answer:


Answer Area
From the Microsoft Entra admin center, create an app registration.
From the Microsoft Purview portal, add the data connector.
Run a sample script to upload File1.csv

by Seidor_Analytics at *Sept. 5, 2025, 8:15 a.m.*

Comments

Eltooth Highly Voted 2 months, 1 week ago

Step 1: Prepare .csv data
Step 2: Create an app registration
Step 3: Add HR data connector
Step 4: Run sample script to upload your HR data

upvoted 5 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 33 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 33

Topic #: 3

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that contains 500 Windows devices.

You plan to deploy Microsoft Purview Data Security Posture Management for AI (DSPM for AI).

You need to ensure that you can monitor user activities on third-party generative AI websites.

Which two prerequisites should you complete for DSPM for AI? Each correct answer presents part of the solution,

NOTE: Each correct selection is worth one point.

A. Create an Endpoint data loss prevention (Endpoint DLP) policy.

B. Onboard the devices to Microsoft Purview. **Most Voted**

C. Install the Microsoft Purview extension on the devices. **Most Voted**

D. Create a communication compliance policy.

E. Enroll the devices in Microsoft Intune.

F. Create a data leaks policy.

Hide Answer

Suggested Answer: *BC*

Community vote distribution

BC (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:18 a.m.*

Comments

Eltooth 2 months, 1 week ago

Selected Answer: BC

B and C are pre-reqs.

upvoted 2 times

RickySmith 2 months, 3 weeks ago

Selected Answer: BC

BC
https://learn.microsoft.com/en-us/purview/dspm-for-ai-considerations#prerequisites-for-data-security-posture-management-for-ai

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 34 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 34

Topic #: 3

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription.

You are implementing insider risk management.

You need to maximize the amount of historical data that is collected when an event is triggered.

What is the maximum number of days that historical data can be collected?

A. 30

B. 60

C. 90 **Most Voted**

D. 180

Hide Answer

Suggested Answer: *C*

Community vote distribution

C (80%) D (20%)

by Seidor_Analytics at *Sept. 5, 2025, 8:25 a.m.*

Comments

Caezarlay 2 months, 2 weeks ago

Selected Answer: C

Given answer is correct.
https://learn.microsoft.com/en-us/purview/insider-risk-management-settings-policy-timeframes

upvoted 4 times

skalolaz 3 months, 1 week ago

Selected Answer: D

It is 180 now.

upvoted 1 times

Gtc_ 2 months, 4 weeks ago

I saw this elsewhere as well, but documentation still states 90 days. Can you link updates?
https://learn.microsoft.com/en-us/purview/insider-risk-management-settings-policy-timeframes

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 35 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 35

Topic #: 3

[All SC-401 Questions]

DRAG DROP

-

You have a Microsoft 365 5 subscription that uses Microsoft Purview insider risk management and contains three users named User1, User2, and User3.

All insider risk management policies have adaptive protection enabled and the default conditions for insider risk levels configured.

The users perform the following activities, which trigger insider risk policy alerts:

- User1 performs at least one data exfiltration activity that results in a high severity risk score.
- User2 performs at least three risky user activities within seven days, that each results in a high severity risk score.
- User3 performs at least two data exfiltration activities within seven days, that each results in a high severity risk score.

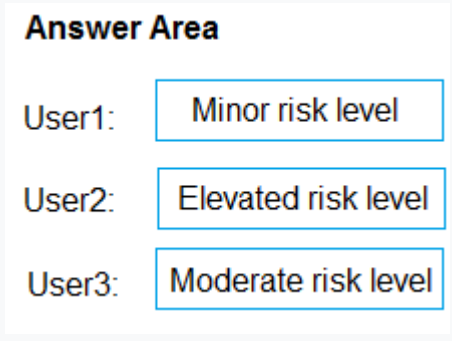
Which insider risk level is assigned to each user? To answer, drag the appropriate levels to the correct users. Each level may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Insider risk levels	Answer Area	
Elevated risk level	User1:	
Minor risk level	User2:	
Moderate risk level	User3:	

Hide Answer

Suggested Answer:



by Seidor_Analytics at *Sept. 5, 2025, 8:24 a.m.*

Comments

Eltooth 2 months, 1 week ago

I would say the answer should be:
Minor (Low)
Elevated (High) - 3 or more high risk scores within 7 days
Elevated (High) - 2 or more data exfiltration activities within 7 days

upvoted 1 times

RickySmith 2 months, 3 weeks ago

Correct
Minor
Elevated
Moderate
https://learn.microsoft.com/en-us/purview/insider-risk-management-adaptive-protection#insider-risk-levels

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 36 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 36

Topic #: 3

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that contains a user named User1.

You need to ensure that all email messages that contain attachments are encrypted automatically by using Microsoft Purview Message Encryption.

What should you create?

A. a mail flow rule **Most Voted**

B. a sensitivity label

C. a data loss prevention (DLP) policy

D. an information barrier segment

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:25 a.m.*

Comments

RickySmith **Highly Voted** 2 months, 3 weeks ago

Selected Answer: A

https://learn.microsoft.com/en-us/purview/define-mail-flow-rules-to-encrypt-email#create-mail-flow-rules-to-encrypt-email-messages-with-microsoft-purview-message-encryption

upvoted 5 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions
View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 37 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 37
Topic #: 3
[All SC-401 Questions]

You have a Microsoft 365 subscription.

You configure a Microsoft Purview insider risk management policy named Policy1.

You need to ensure that you will receive real-time recommendations on how to configure the indicator thresholds for Policy1. The solution must ensure that the recommendations are based on a user's activity from the past 10 days.

What should you do first?

A. Create an Insider Risk Indicators connector.

B. Configure the Insider Risk Management Data sharing settings.

C. Create a data loss prevention (DLP) policy

D. Enable insider risk management analytics. **Most Voted**

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:18 a.m.*

Comments

Eltooth 2 months, 1 week ago

Selected Answer: D

D is correct answer.

To receive real-time recommendations on how to configure indicator thresholds for an Insider Risk Management policy (like Policy1), you must first enable Insider Risk Management analytics.
Insider risk analytics provides insights into user activities and helps identify potential risks before creating or tuning policies. It analyzes user activity from the past 10 days and offers recommendations for configuring thresholds and identifying high-risk users.

upvoted 3 times

RickySmith 2 months, 3 weeks ago

Selected Answer: D

https://learn.microsoft.com/en-us/purview/insider-risk-management-settings-policy-indicators#use-real-time-analytics-recommendations-to-set-thresholds

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 38 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 38

Topic #: 3

[All SC-401 Questions]

DRAG DROP

-

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

You need to implement insider risk management. The solution must meet the following requirements:

- Ensure that User1 can create insider risk management policies.
- Ensure that User2 can use content captured by using insider risk management policies.
- Follow the principle of least privilege.

To which role group should you add each user? To answer, drag the appropriate role groups to the correct users. Each role group may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Role groups

- Insider Risk Management
- Insider Risk Management Admins
- Insider Risk Management Analysts
- Insider Risk Management Auditors
- Insider Risk Management Investigators

Answer Area

User1:

User2:

Hide Answer

Suggested Answer:

by Seidor_Analytics at *Sept. 5, 2025, 8:16 a.m.*

Comments

RickySmith Highly Voted 2 months, 3 weeks ago

Admins
Investigators
https://learn.microsoft.com/en-us/purview/insider-risk-management-permissions

upvoted 7 times

Eltooth Most Recent 2 months ago

Admins
Investigators - they can access content captured by IRM policies, however limited to assigned cases. Cannot see all alerts or manage cases broadly.

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 39 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 39

Topic #: 3

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft Purview insider risk management.

You need to recommend policy templates that meet the following requirements:

- Contain risk indicators and scoring for when a user receives a poor performance review.
- Contain risk indicators and scoring for when a user disables security features on a device.

Which template should you use for each requirement? To answer, select the appropriate options in the answer area,

NOTE: Each correct selection is worth one point.

Answer Area

When a user receives a poor performance review:

- Data leaks
- Data theft by departing users
- Security policy violations
- Security policy violations by risky users

When a user disables security features:

- Data leaks
- Data theft by departing users
- Security policy violations
- Security policy violations by risky users

Hide Answer

Suggested Answer:

Answer Area

When a user receives a poor performance review:

- Data leaks
- Data theft by departing users
- Security policy violations
- **Security policy violations by risky users**

When a user disables security features:

- Data leaks
- Data theft by departing users
- **Security policy violations**
- Security policy violations by risky users

by Seidor_Analytics at *Sept. 5, 2025, 8:16 a.m.*

Comments

RickySmith Highly Voted 2 months, 2 weeks ago

Given response is correct.
Security policy violations by risky users
Security policy violations
https://learn.microsoft.com/en-us/purview/import-hr-data#step-1-prepare-a-csv-file-with-your-hr-data

upvoted 5 times

Eltooth Most Recent 2 months, 3 weeks ago

Data theft by departing users
Security policy violations

Recommended Template: "Departing Employee"
Why:
This template includes HR signals such as poor performance reviews, termination, or resignation.
It uses risk indicators and scoring based on HR data imported via Microsoft Entra ID or HR connector integrations.

Recommended Template: "Security Policy Violations"
Why:
This template includes indicators for device-related risky behavior, such as disabling antivirus, firewall, or other security controls.
It monitors for violations of organizational security policies.

upvoted 1 times

Eltooth 2 months ago

Corrrection - Data Theft by departing users is wrong. The correct Template for Poor Performance Review should be:
Security policy violations by risky users
Detects security violations by users whose activity might be risky based on messages they send or having experienced a stressor event, such as a poor performance review. Includes activity generated by Microsoft Defender for Endpoint alerts, which detect possible security violations performed on devices.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 40 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 40

Topic #: 3

[All SC-401 Questions]

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You have a user named User1. Several users have full access to the mailbox of User1.

Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in the Microsoft Purview portal to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1.

Solution: You run the Set-AuditConfig –Workload Exchange command.

Does that meet the goal?

A. Yes **Most Voted**

B. No

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (75%) A (25%)

by Seidor_Analytics at *Sept. 5, 2025, 8:16 a.m.*

Comments

Eltooth 2 months, 1 week ago

Selected Answer: B

B is correct answer: No.
This command enables auditing at the organization level for Exchange, but does not enable auditing on individual mailboxes if it's not already turned on.
To capture delegate mailbox access, mailbox-level auditing must be enabled and configured with the appropriate actions.

To ensure that future mailbox sign-ins (including delegate access) are audited and visible in the Microsoft Purview audit logs, you need to:
Enable mailbox auditing for User1
As of recent updates, mailbox auditing is enabled by default for all users in Microsoft 365. However, if it's not enabled or was disabled, you must explicitly enable it:
Set-Mailbox -Identity "User1" -AuditEnabled $true
Set-Mailbox -Identity "User1" -AuditDelegate SendOnBehalf, SendAs, Update, SoftDelete, HardDelete, MoveToDeletedItems, Copy, MessageBind

upvoted 3 times

Alcpt 3 weeks, 5 days ago

The Set-AuditConfig –Workload Exchange command alone will not meet the goal because:
Mailbox auditing must be enabled at the mailbox level for User1, not just at the workload level
The correct approach would be to enable mailbox auditing specifically for User1's mailbox using:
Set-Mailbox -Identity User1 -AuditEnabled $true

upvoted 1 times

RickySmith 2 months, 2 weeks ago

Selected Answer: A

https://learn.microsoft.com/en-us/powershell/module/exchangepowershell/set-auditconfig?view=exchange-ps

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 41 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 41

Topic #: 3

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.

You need to deploy a Microsoft Purview insider risk management solution that will generate an alert when users share sensitive information on Site1 with external recipients.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct answer is worth one point.

A. Turn on analytics.

B. Turn on indicators. **Most Voted**

C. Configure adaptive protection.

D. Create an insider risk policy. **Most Voted**

E. Create a data loss prevention (DLP) policy.

Hide Answer

Suggested Answer: *BD*

Community vote distribution

BD (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:17 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

Selected Answer: BD

B. Turn on indicators
Indicators are the core signals used to detect risky activities, such as sharing sensitive data externally.
You must enable relevant indicators like "Sharing of sensitive information" to trigger alerts.

D. Create an insider risk policy

Insider risk policies define who is monitored, what activities are tracked, and what thresholds trigger alerts.
You need to create a policy that includes:
The appropriate indicator (e.g., data sharing).
The sensitive info types or sensitivity labels.
The scope of users/sites involved.

upvoted 3 times

Eltooth 2 months, 1 week ago

Note - you dont need DLP policy to enable this feature as you can skip sensitivity labels, SITs, trainable classifiers & file extensions. You can simply add SharePoint site and triggering action: "Sharing SharePoint files with people outside my org"

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 42 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 42

Topic #: 3

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that contains a user named User1.

You deploy Microsoft Purview insider risk management.

You need ensure that insider risk management events related to User1 are visible only to specific users.

What should you create?

A. a detection group

B. a global exclusion

C. an indicator variant

D. a priority user group **Most Voted**

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:17 a.m.*

Comments

RickySmith 2 months, 2 weeks ago

Selected Answer: D

D
https://learn.microsoft.com/en-us/purview/insider-risk-management-settings-priority-user-groups#create-a-priority-user-group
"11.On the Choose who can view this group page..."

upvoted 3 times

Eltooth 2 months, 3 weeks ago

Selected Answer: D

D is correct answer.

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 43 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 43

Topic #: 3

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 E5 subscription.

You plan to use the Microsoft Purview portal to map human resources (HR) data for use with insider risk management policies.

You need to add a data connector to import the HR data.

What should you do first, and in which format should you import the data? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

First:

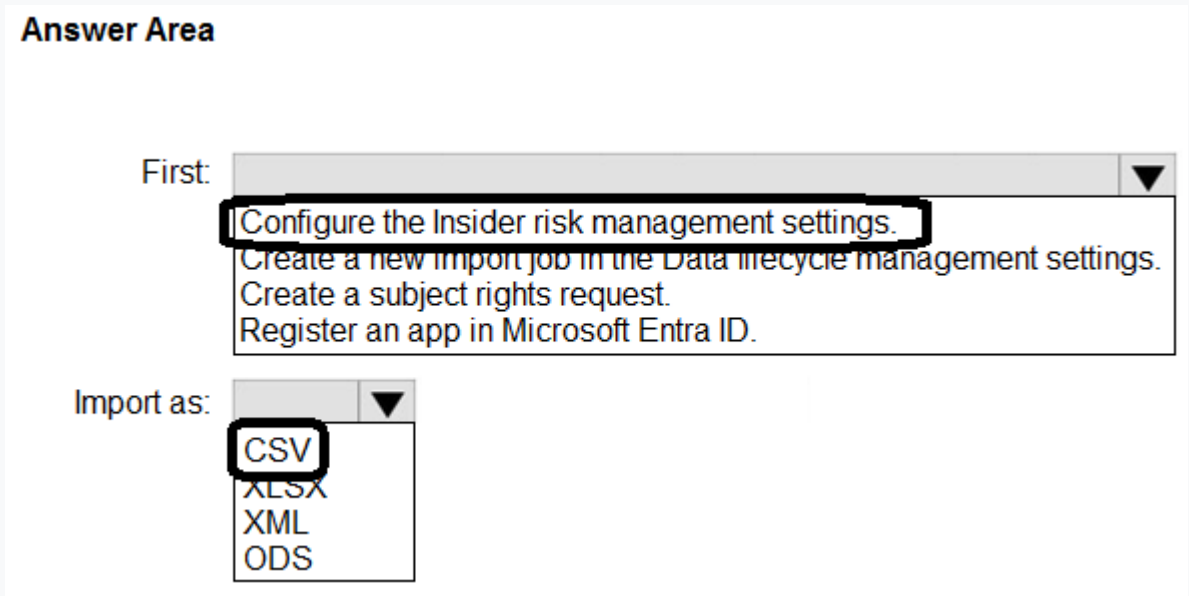
- Configure the Insider risk management settings.
- Create a new import job in the Data lifecycle management settings.
- Create a subject rights request.
- Register an app in Microsoft Entra ID.

Import as:

- CSV
- XLSX
- XML
- ODS

Hide Answer

Suggested Answer:



by Seidor_Analytics at *Sept. 5, 2025, 8:17 a.m.*

Comments

RickySmith Highly Voted 2 months, 3 weeks ago

4,1
https://learn.microsoft.com/en-us/purview/import-hr-data
upvoted 10 times

Eltooth Most Recent 2 months, 3 weeks ago

Step 1: Prepare a CSV file with your HR data
Step 2: Create an app in Microsoft Entra ID
Step 3: Create the HR connector
Step 4: Run the sample script to upload your HR data
Step 5: Monitor the HR connector
(Optional) Step 6: Schedule the script to run automatically
(Optional) Step 7: Upload data by using Power Automate templates
upvoted 3 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 44 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 44
Topic #: 3
[All SC-401 Questions]

HOTSPOT
-

You have a Microsoft 365 E5 subscription.

You need to ensure that users are prevented from uploading sensitive data to ChatGPT and Google Gemini. The solution must meet the following requirements:

- Prevent credit card numbers from being pasted into ChatGPT and Gemini.
- Prevent documents that contain classified data from being uploaded to ChatGPT and Gemini.

Which Microsoft Purview solution should you use for each requirement? To answer, select the appropriate options in the answer

NOTE: Each correct selection is worth one point.

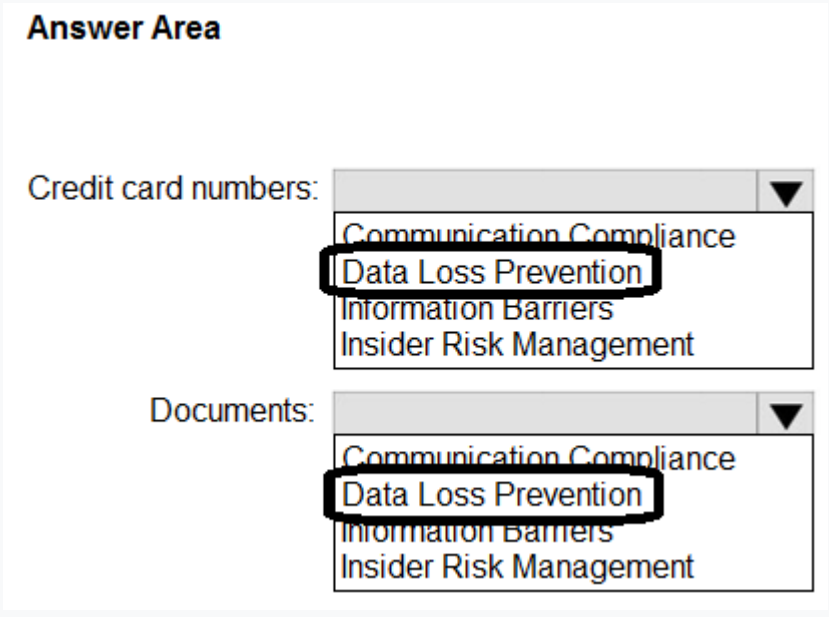
Answer Area

Credit card numbers:
- Communication Compliance
- Data Loss Prevention
- Information Barriers
- Insider Risk Management

Documents:
- Communication Compliance
- Data Loss Prevention
- Information Barriers
- Insider Risk Management

Hide Answer

Suggested Answer:



by Gtc_ at *Sept. 2, 2025, 10:56 p.m.*

Comments

RickySmith 2 months, 3 weeks ago

Data Loss Prevention
https://learn.microsoft.com/en-us/purview/ai-microsoft-purview#data-loss-prevention-and-ai-interactions

upvoted 4 times

Gtc_ 3 months, 1 week ago

Correct

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 45 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 45

Topic #: 3

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 E5 subscription.

You are implementing insider risk management.

You need to create an insider risk management notice template and format the message body of the notice template.

How should you configure the template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Use the:

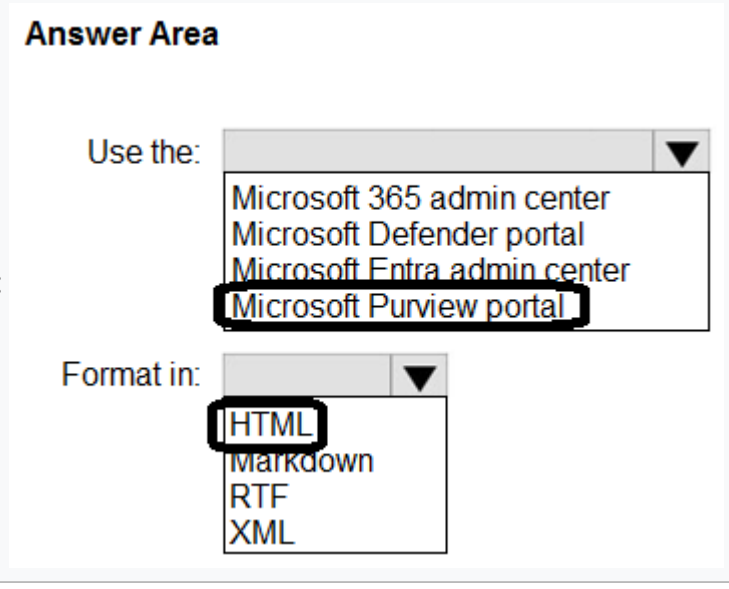
- Microsoft 365 admin center
- Microsoft Defender portal
- Microsoft Entra admin center
- Microsoft Purview portal

Format in:

- HTML
- Markdown
- RTF
- XML

Hide Answer

Suggested Answer:



by Gtc_ at *Sept. 2, 2025, 10:55 p.m.*

Comments

Eltooth 2 months, 3 weeks ago

Purview
HTML
upvoted 4 times

Gtc_ 3 months, 1 week ago

Correct
upvoted 2 times

RickySmith 2 months, 3 weeks ago

https://learn.microsoft.com/en-us/purview/insider-risk-management-notices
upvoted 1 times

RickySmith 2 months, 2 weeks ago

https://learn.microsoft.com/en-us/purview/insider-risk-management-notices#create-a-new-notice-template
upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 46 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 46

Topic #: 3

[All SC-401 Questions]

SIMULATION

-

Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and select the username below.

To enter your password, place your cursor in the Enter password box and select the password below.

Microsoft 365 Username:
admin@WWLx971455.onmicrosoft.com

Microsoft 365 Password: XXXXXXXXX

If the Microsoft Edge browser or Microsoft 365 portal does not load successfully, select the Microsoft Edge browser icon from the task bar, type the URL “https://admin microsoft.com”, and press Enter.

The following information is for technical support purposes only:
Lab Instance: XXXXXXXX.

Task 8

-

You need to create a retain Microsoft SharePoint files that contain the word Falcon for two years from the date they were created and then delete them.

Hide Answer

Suggested Answer:

Plan:
Stage 1: Create custom sensitive information types in the Microsoft Purview compliance portal
Stage 2: Create retention policy and use the sensitive info type created in stage 1

Stage 1: Create custom sensitive information types in the Microsoft Purview compliance portal

Create a custom SIT from scratch

Step 1: Use the following procedure to fully define a brand new sensitive information type.

Step 2: In the Microsoft Purview compliance portal, navigate to Data classification > Classifiers > Sensitive info types and choose Create sensitive info type.

Step 3: Fill in values for Name and Description and choose Next.

Step 4: Choose Create pattern. You can create multiple patterns, each with different elements and confidence levels, as you define your new sensitive information type.

Step 5: Choose the default confidence level for the pattern. The values are Low confidence, Medium confidence, and High confidence.

Step 6: Choose and define the Primary element. Choose Keyword list.

Step 7: Enter: Falcon

Question: You need to retain Microsoft SharePoint files that contain the word Falcon for two years from the date they were created, and then delete them.

Step 8: Finish the wizard.

Stage 2: Create retention policy and use the sensitive info type created in stage 1

Step 1: From the Microsoft Purview compliance portal, select Data lifecycle management > Microsoft 365 > Retention Policies.

Step 2: Select New retention policy to start the Create retention policy configuration, and name your new retention policy.

Step 3: For the Assign admin units page select Full directory.
You must select Full directory for the policy to include the locations for SharePoint sites and Exchange public folders.

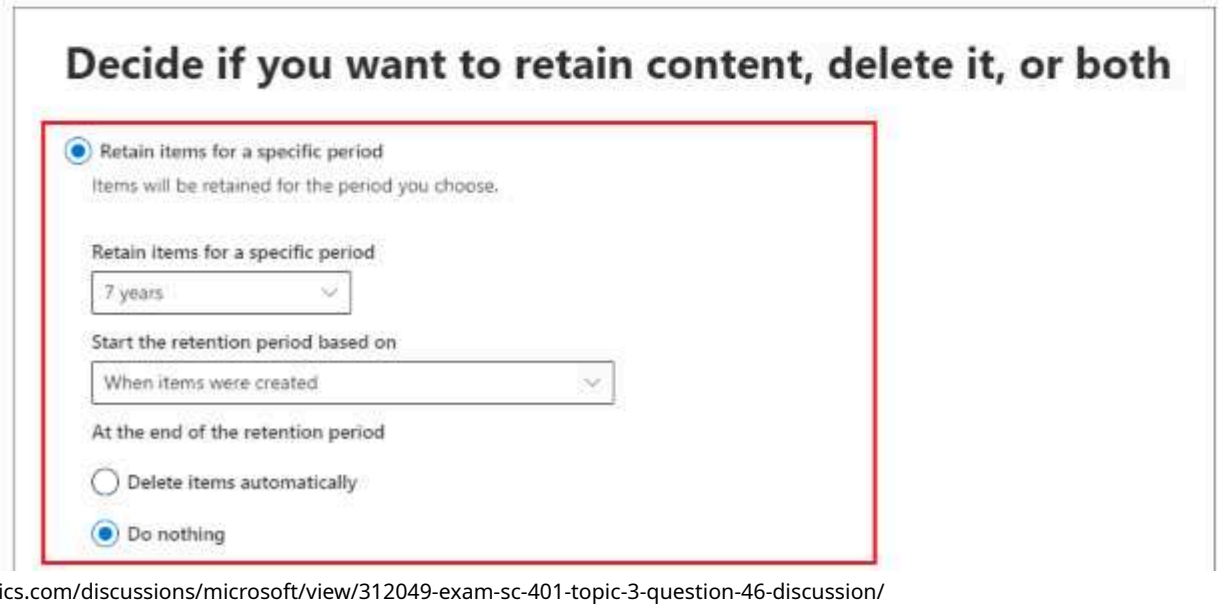
Step 4: For the Choose the type of retention policy to create page, select Adaptive or Static. Select Static.

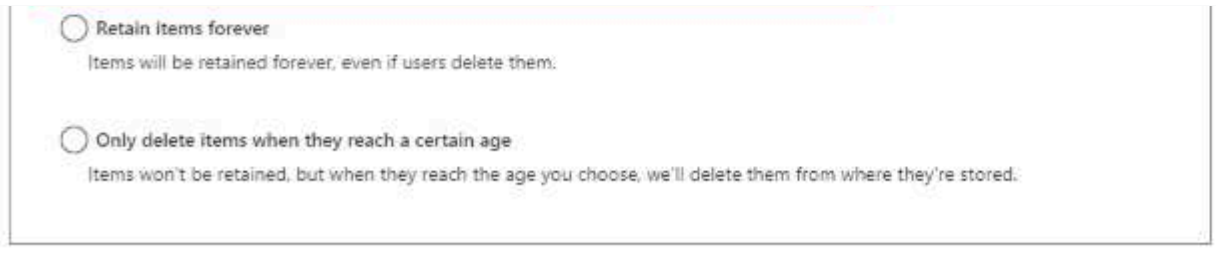
Step 5: For location: Select Items, and Sharepoint

Step 6: Somehow include the sensitive information type you created in Stage 1.

Step 7: For Decide if you want to retain content, delete it:
Select: On the Decide if you want to retain content, delete it, or both page, select Retain items for a specific period, specify the retention period [specify 2 years], and then for At end of the retention period select Delete items automatically.

Question: You need to retain Microsoft SharePoint files that contain the word Falcon for two years from the date they were created, and then delete them.


Decide if you want to retain content, delete it, or both
Retain items for a specific period
Items will be retained for the period you choose.
Retain items for a specific period
7 years
Start the retention period based on
When items were created
At the end of the retention period
Delete items automatically
Do nothing


Retain items forever
Items will be retained forever, even if users delete them.
Only delete items when they reach a certain age
Items won't be retained, but when they reach the age you choose, we'll delete them from where they're stored.

Reference:
https://learn.microsoft.com/en-us/purview/sit-create-a-custom-sensitive-information-type
https://learn.microsoft.com/en-us/purview/create-retention-policies
https://learn.microsoft.com/en-us/purview/retention-settings#settings-for-retaining-and-deleting-content

by Seidor_Analytics at *Sept. 5, 2025, 8:25 a.m.*

Comments

bobg 2 weeks, 3 days ago

Create a SIT and then create an Auto Labelling Retention Policy checking for that SIT.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 47 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 47

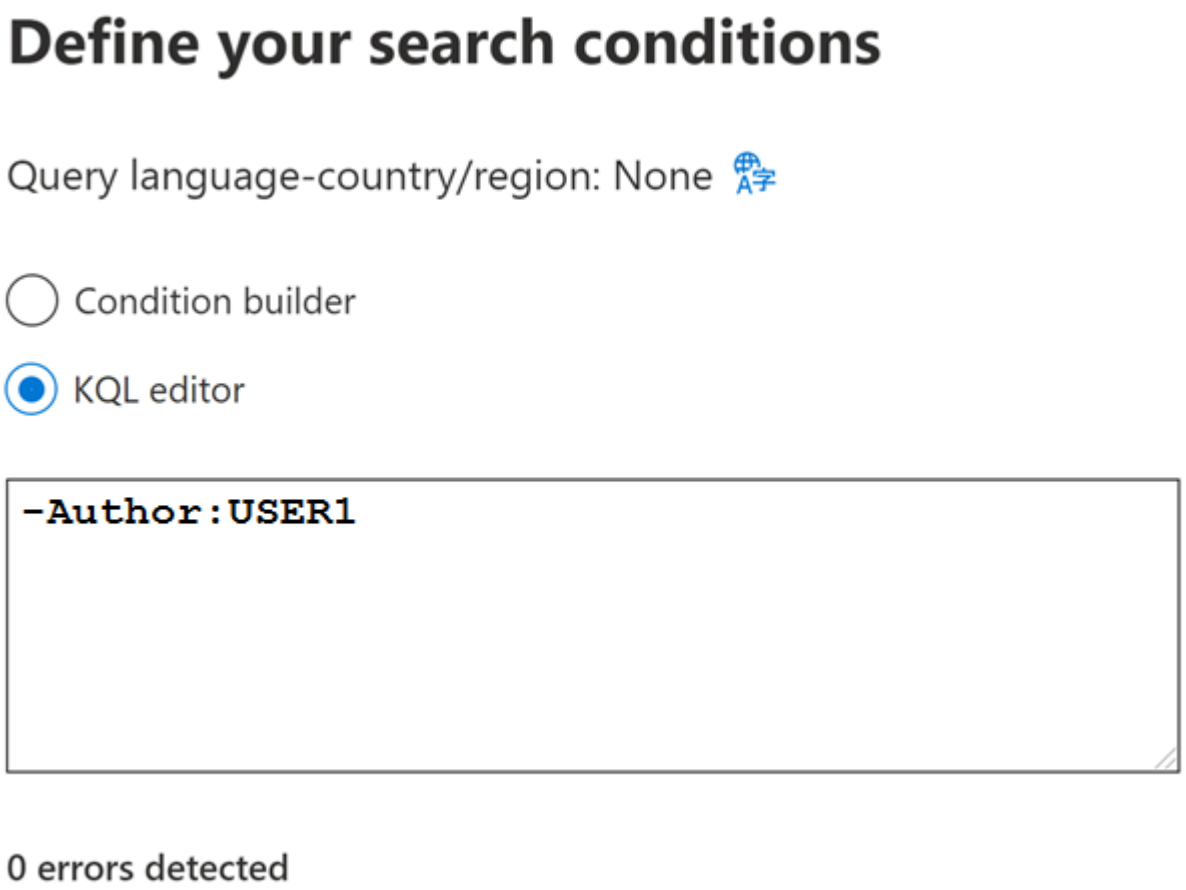
Topic #: 3

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 contains the files shown in the following table.

Name	Author
File1.docx	User1
File2.docx	User2
File3.docx	USER1

In the Microsoft Purview portal, you create a content search named Content1 and configure the search conditions as shown in the following exhibit.



Which files will be returned by Content1?

A. File2.docx only

B. File3.docx only

C. File1.docx and File2.docx only

D. File1.docx and File3.docx only **Most Voted**

E. Filet.docx, File2.docx, and File3.docx

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:23 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

Selected Answer: D

"-" is ignored by KeyQL. Author: looks for all files created by USER1.
Therefore File1 and File 3 are returned.
https://learn.microsoft.com/en-gb/purview/edisc-condition-builder#special-characters

upvoted 2 times

bobg 2 weeks, 3 days ago

I think its A. The - still stands as NOT. The note on that website only applies if it was part of the search query i think. For example USER-1. I'm not 100% sure though.

upvoted 1 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 48 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 48

Topic #: 3

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription.

You plan to use insider risk management to collect and investigate forensic evidence.

You need to enable forensic evidence capturing.

What should you do first?

A. Configure the information protection scanner.

B. Claim capacity **Most Voted**

C. Enable Adaptive Protection

D. Create priority user groups.

Hide Answer

Suggested Answer: *B*

Community vote distribution

B (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:16 a.m.*

Comments

Eltooth 2 months, 3 weeks ago

Selected Answer: B

B is correct answer : Claim Capacity.
https://learn.microsoft.com/en-us/purview/insider-risk-management-forensic-evidence-configure#step-1-confirm-your-subscription-and-configure-data-storage-access

upvoted 2 times

florinvele 2 months, 4 weeks ago

Selected Answer: B

First you claim the capacity

upvoted 2 times

Gtc_ 2 months, 4 weeks ago

Selected Answer: B

Correct. forensic evidence capture in Insider Risk Management requires you to claim capacity in the purview portal before you can enable it. this reserves capacity in your tenant for storing and analyzing forensic artifacts

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 49 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 49

Topic #: 3

[All SC-401 Questions]

You have a Microsoft 365 subscription.

You create and run a content search from the Microsoft Purview portal.

You need to download the results of the content search.

What should you obtain first?

A. a certificate

B. a password

C. a pin

D. an export key **Most Voted**

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:16 a.m.*

Comments

RickySmith 2 months, 3 weeks ago

Selected Answer: D

https://learn.microsoft.com/en-us/purview/ediscovery-export-search-results#step-2-download-the-search-results

upvoted 2 times

florinvele 2 months, 4 weeks ago

Selected Answer: D

Export key

upvoted 2 times

Gtc_ 2 months, 4 weeks ago

Selected Answer: D

correct answer

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 50 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 50

Topic #: 3

[All SC-401 Questions]

You have a Microsoft 365 tenant that uses Microsoft Purview Message Encryption.

You need to ensure that any emails containing attachments and sent to user1@contoso.com are encrypted automatically by using Microsoft Purview Message Encryption.

What should you do?

A. From the Exchange admin center, create a mail flow rule. **Most Voted**

B. From the Exchange admin center, create a new sharing policy.

C. From the Microsoft Defender portal, create a Safe Attachments policy.

D. From the Microsoft Purview portal, configure an auto-apply retention label policy.

Hide Answer

Suggested Answer: *A*

Community vote distribution

A (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:17 a.m.*

Comments

Gtc_ 2 months, 4 weeks ago

Selected Answer: A

OME in Exchange Admin Center

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 51 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 51

Topic #: 3

[All SC-401 Questions]

You have a Microsoft 365 subscription linked to a Microsoft Entra tenant that contains a user named User1.

You need to grant User1 permission to search Microsoft 365 audit logs. The solution must use the principle of least privilege.

Which role should you assign to User?

A. the Compliance Management role in the Exchange admin center

B. the Security Reader role in the Microsoft Entra admin center

C. the View-Only Audit Logs role in the Exchange admin center **Most Voted**

D. the Reviewer role in the Microsoft Purview portal

Hide Answer

Suggested Answer: *C*

Community vote distribution

C (100%)

by Seidor_Analytics at *Sept. 5, 2025, 8:17 a.m.*

Comments

Eltooth 2 months, 2 weeks ago

Selected Answer: C

C feels the least privileged role between that and Security reader

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 53 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 53

Topic #: 3

[All SC-401 Questions]

HOTSPOT

-

You have a Microsoft 365 E5 subscription.

From the Microsoft Purview Data Security Posture Management for AI portal, you review the recommendations for AI data security.

You plan to create a one-click policy to block elevated risk users from pasting or uploading sensitive data to AI websites.

How will the policy be configured? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

The policy mode will be configured to use:

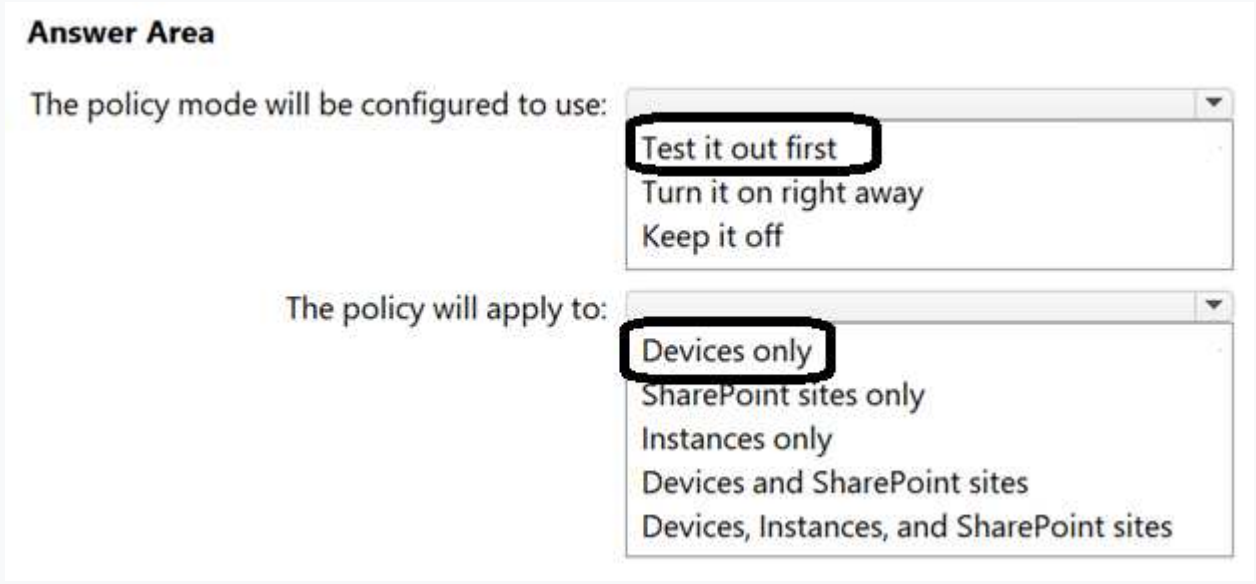
- Test it out first
- Turn it on right away
- Keep it off

The policy will apply to:

- Devices only
- SharePoint sites only
- Instances only
- Devices and SharePoint sites
- Devices, Instances, and SharePoint sites

Hide Answer

Suggested Answer:



by Alcpt at *Nov. 18, 2025, 7:49 a.m.*

Comments

Alcpt 3 weeks, 5 days ago

I would choose 2 & 5,
For a one-click policy designed to immediately block risky behavior, "Turn it on right away" is appropriate rather than testing or keeping it off.

Since the policy aims to prevent data exfiltration to AI websites, it needs to cover multiple scopes: Devices (to block local actions), Instances (AI service instances), and SharePoint sites (where sensitive data might be stored).

upvoted 4 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 54 DISCUSSION

Actual exam question from Microsoft's SC-401
Question #: 54
Topic #: 3
[All SC-401 Questions]

You have a Microsoft 365 E5 subscription.

You plan to use Microsoft Purview insider risk management.

You need to create an insider risk management policy that will detect data theft from Microsoft SharePoint Online by users that submitted their resignation or are near their employment termination date.

What should you do first?

A. Configure Office indicators.

B. Onboard devices to Microsoft Defender for Endpoint.

C. Configure a Physical badging connector.

D. Configure a HR data connector. **Most Voted**

Hide Answer

Suggested Answer: *D*

Community vote distribution

D (100%)

by Alcpt at *Nov. 18, 2025, 7:52 a.m.*

Comments

Alcpt 3 weeks, 5 days ago

Selected Answer: D

D. Configure a HR data connector.
Here's why:
To detect data theft by users who have resigned or are near their termination date, Microsoft Purview Insider Risk Management needs access to HR signals (such as resignation date or termination date). These signals come from your HR system and are ingested through an HR data connector. Without this connector, the policy cannot identify which users are at risk based on employment status.

upvoted 2 times

EXAMTOPICS

Microsoft Discussions

Exam SC-401 All Questions

View all questions & answers for the SC-401 exam

Go to Exam

EXAM SC-401 TOPIC 3 QUESTION 57 DISCUSSION

Actual exam question from Microsoft's SC-401

Question #: 57

Topic #: 3

[All SC-401 Questions]

You have a Microsoft 365 E5 subscription that contains a user named User1.

All users are assigned Microsoft 365 Copilot licenses.

You deploy Microsoft Purview Data Security Posture Management for AI (DSPM for AI).

You need to ensure that User1 can analyze prompts and responses for AI interaction events. The solution must follow the principle of least privilege.

To which two role groups should you add User1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Security Reader

B. Content Explorer List Viewer

C. Insider Risk Management Investigators

D. Information Protection Analysts

E. Content Explorer Content Viewer

Hide Answer

Suggested Answer: *AE*

Community vote distribution

DE (100%)

by Pavol_Misun at *Nov. 12, 2025, 1:16 p.m.*

Comments

Pavol_Misun 1 month ago

Selected Answer: DE

D. Information Protection Analysts
E. Content Explorer Content Viewer

E. Content Explorer Content Viewer: By default, an analyst can only see the metadata about an event (like the user, date, and policy it violated). They cannot read the actual content of the prompt or response due to privacy rules. To "analyze prompts and responses," User1 needs this specific role, which grants permission to open and read the content of items within the Content Explorer.

upvoted 2 times